CyberAGI VOL 2 Part 2

1 message

DANISH KHAN <danishkhanlko@gmail.com> Wed, 24 Jan, 2024 at 4:55 am
Draft

What is Encryption ?

Encryption is a process of transforming data into an unreadable form, so that only authorized parties can access and understand it. Encryption is important for ensuring the security and privacy of data, especially in edge computing, where data is generated and processed on devices that are closer to the users, such as smartphones, tablets, laptops, or IoT sensors[1].

There are different ways of implementing encryption in edge computing, depending on the type and purpose of the data, the capabilities and constraints of the devices, and the level of security and efficiency required. Some of the common methods are:

- **Symmetric encryption**: This is a method where the same key is used to encrypt and decrypt the data. Symmetric encryption is fast and simple, but it requires a secure way of distributing and storing the key among the devices. Symmetric encryption can be used for encrypting data at rest or in transit on edge devices[2].
- **Asymmetric encryption**: This is a method where two different keys are used to encrypt and decrypt the data: a public key and a private key. The public key can be shared with anyone, while the private key is kept secret by the owner. Asymmetric encryption is more secure and flexible than symmetric encryption, but it is also more complex and slower. Asymmetric encryption can be used for authenticating and verifying the identity of the devices, as well as encrypting sensitive or confidential data[2].
- **Attribute-based encryption**: This is a method where the data is encrypted based on a set of attributes or policies, rather than a specific key. The data can only be decrypted by the devices that satisfy the attributes or policies. Attribute-based encryption can provide fine-grained access control and privacy protection for data on edge devices, as well as support keyword search and revocation functions[3].
- **Homomorphic encryption**: This is a method where the data can be processed or analyzed without decrypting it first. Homomorphic encryption can enable edge devices to perform computations on encrypted data, such as aggregation or filtering, without revealing the original data or compromising its security. Homomorphic encryption can reduce the communication and storage overhead of edge devices, as well as enhance their privacy and efficiency[4].

Therefore, encryption works in edge computing by using different methods to protect the data from unauthorized or malicious access, while enabling its processing and analysis on edge devices.

Source: Conversation with Bing, 9/4/2023
(1) An efficient and secure aggregation encryption scheme in edge computing .... https://ieeexplore.ieee.org/document/9745440/.
(2) Attribute-Based Searchable Encryption in Edge Computing for Lightweight .... https://ieeexplore.ieee.org/document/10175644/.
(3) A context-aware encryption protocol suite for edge computing-based IoT .... https://link.springer.com/article/10.1007/s11227-019-03021-2.
(4) Edge Encryption - Data Encryption - ServiceNow. https://www.servicenow.com/products/edge-encryption.html.
(5) undefined. https://ieeexplore.ieee.org/servlet/opac?punumber=6245522.
(6) undefined. https://ieeexplore.ieee.org/servlet/opac?punumber=4267003.

Data quality and Cybersecurity for devices Leveraging Edge Computing Technology ?

Data quality on edge devices is important for ensuring reliable and robust AI applications on the edge. There are some ways to improve the data quality on edge devices, such as:

- **Analyze the right data at the edge**: The first step to improving data processing at the edge is focusing on the correct data to process on edge devices. Not all data needs to be processed at the edge, and some data may be better suited for cloud or data center processing. Edge devices should analyze the data that is most relevant, timely, and critical for the application, and filter out the unnecessary or redundant data[3].
- **Investigate data before storing it**: Edge processing is all about removing the time and bandwidth required to send information to the cloud or a data center to process it. However, this also means that edge devices need to store the processed data locally, which can consume valuable memory and storage space. Therefore, edge devices should investigate the data before storing it, and determine whether it is worth keeping, deleting, or sending to the cloud for further analysis[3].
- **Strengthen security**: Edge devices are more vulnerable to cyberattacks, data breaches, or physical tampering, which can compromise the security and privacy of the data and the AI models. Edge devices need to implement strong encryption, authentication, and access control mechanisms to protect the data and the AI models from unauthorized or malicious access[1][2].

Some of the challenges of using edge computing with AI are:

- **Poor data quality**: Edge devices may generate noisy, incomplete, or inaccurate data, which can affect the performance and accuracy of AI models. Data quality management and validation are essential for ensuring reliable and robust AI applications on the edge[4].
- **Limited resources**: Edge devices have limited computing power, memory, storage, and battery life, which can constrain the complexity and efficiency of AI models. AI models need to be optimized and compressed to fit the resource constraints of edge devices, without compromising their functionality and quality[1][2].
- **Security and privacy**: Edge devices are more vulnerable to cyberattacks, data breaches, or physical tampering, which can compromise the security and privacy of the data and the AI models. Edge devices need to implement strong encryption, authentication, and access control mechanisms to protect the data and the AI models from unauthorized or malicious access[1][3].
- **Network connectivity**: Edge devices rely on network connectivity to communicate with each other and with the cloud, which can be unstable, intermittent, or unavailable in some scenarios. Edge devices need to be able to operate offline or with low bandwidth, and synchronize with the cloud when possible[1][2]..

Source: Conversation with Bing, 9/4/2023
(1) Edge AI: The Future of Artificial Intelligence and Edge Computing. https://www.itbusinessedge.com/data-center/developments-edge-ai/.
(2) Edge AI Explained: How It Works, Features, Challenges & More. https://www.splunk.com/en_us/blog/learn/edge-ai.html.
(3) Edge Computing and AI for IoT: Opportunities and Challenges. https://ieeexplore.ieee.org/abstract/document/10226787.
(4) Artificial intelligence: a killer app for edge computing?. https://stlpartners.com/articles/edge-computing/artificial-intelligence-a-killer-app-for-edge-computing/.
(5) undefined. https://ieeexplore.ieee.org/servlet/opac?punumber=10226627.
(6) Getty Images. https://www.gettyimages.com/detail/photo/edge-computing-technology-with-distributed-network-royalty-free-image/1197264259.

Source: Conversation with Bing, 9/4/2023
(1) What are the Best Ways to Improve Data Processing at the Edge?. https://itchronicles.com/big-data/what-are-the-best-ways-to-improve-data-processing-at-the-edge/.
(2) A blockchain-based framework for data quality in edge ... - Springer. https://link.springer.com/article/10.1007/s11704-022-2083-8.
(3) Adaptive Strategy to Improve the Quality of Communication for IoT Edge .... https://ieeexplore.ieee.org/document/9221276/.

(4) What is edge computing? | IBM. https://www.ibm.com/topics/edge-computing.
(5) undefined. https://ieeexplore.ieee.org/servlet/opac?punumber=9217527.

Most AI LLMs can switch between cloud computing and edge computing depending on the availability of seamless fast networks, but this requires some optimization and adaptation from the developers and the devices. Some practical examples are:

- **Microsoft Office 365 Co-pilot**: This is a feature that uses AI to help users across the Windows OS. It uses AI hardware in both the cloud and locally, where possible, to run LLMs for tasks such as writing assistance, image generation, and data analysis[1].
- **Apple Siri**: This is a voice assistant that uses AI to answer questions and perform actions. It uses cloud computing for most of its functions, but it also uses edge computing for some tasks that require low latency or privacy, such as speech recognition, device control, and offline mode[2].
- **Google Assistant**: This is another voice assistant that uses AI to provide various services. It also uses cloud computing for most of its features, but it can use edge computing for some functions that need speed or security, such as voice commands, smart home control, and driving mode[3].

Source: Conversation with Bing, 9/4/2023
(1) How To Run Large AI Models On An Edge Device - Forbes. https://www.forbes.com/sites/karlfreund/2023/07/10/how-to-run-large-ai-models-on-an-edge-device/.
(2) Qualcomm Is Right About AI: It Requires Strong Edge Computing - Forbes. https://www.forbes.com/sites/patrickmoorhead/2023/06/27/qualcomm-is-right-about-ai-it-requires-strong-edge-computing/.
(3) Cloud AI, Edge AI, Endpoint AI. What's the Difference? - Arm. https://www.arm.com/blogs/blueprint/cloud-edge-endpoint-ai.
(4) AI and ML in edge computing: Benefits, applications, and how they're .... https://blog.shi.com/next-generation-infrastructure/ai-and-ml-in-edge-computing/.

Edge computing works with AI by running AI algorithms on local devices that have edge computing capabilities. This means that the data can be processed in real-time, without having to connect to a cloud or a central server. Edge computing can enable AI applications to run on devices such as smartphones, tablets, laptops, or IoT sensors, without relying on the cloud[3][4]. Some of the benefits of edge computing for AI are:

- **Reduced latency**: Edge computing can provide faster data processing and analysis, as the data does not have to travel to the cloud and back. This can improve the performance of AI applications that require real-time or near-real-time feedback, such as autonomous vehicles, facial recognition, or voice assistants.
- **Enhanced security**: Edge computing can reduce the risk of data breaches, as the data is stored and processed locally on the device, rather than on a remote server. This can protect sensitive or personal data from unauthorized access or manipulation.
- **Lower cost**: Edge computing can reduce the cost of data transmission and storage, as less data is sent to the cloud. This can save bandwidth and network resources, and lower the dependency on cloud service providers.

Therefore, edge computing works with AI by providing faster, more secure, and more cost-effective data processing and analysis..

Source: Conversation with Bing, 9/4/2023
(1) What Edge AI & Edge Computing? - Unite.AI. https://www.unite.ai/what-is-edge-ai/.
(2) Complete Guide to Edge Computing, Edge IoT, Edge AI & More - Run. https://www.run.ai/guides/edge-computing.
(3) What Is Edge AI and How Does It Work? | NVIDIA Blog. https://blogs.nvidia.com/blog/2022/02/17/what-is-edge-ai/.
(4) Edge AI: The Future of Artificial Intelligence and Edge Computing. https://www.itbusinessedge.com/data-center/developments-edge-ai/.
(5) Getty Images. https://www.gettyimages.com/detail/photo/edge-computing-technology-with-distributed-network-royalty-free-image/1197264259.

AI can leverage its performance in the absence of high-speed cloud computing network by using **edge computing**. Edge computing is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth. Edge computing can enable AI applications to run on devices such as smartphones, tablets, laptops, or IoT sensors, without relying on the cloud. Some of the benefits of edge computing for AI are:

- **Reduced latency**: Edge computing can provide faster data processing and analysis, as the data does not have to travel to the cloud and back. This can improve the performance of AI applications that require real-time or near-real-time feedback, such as autonomous vehicles, facial recognition, or voice assistants.
- **Enhanced security**: Edge computing can reduce the risk of data breaches, as the data is stored and processed locally on the device, rather than on a remote server. This can protect sensitive or personal data from unauthorized access or manipulation.
- **Lower cost**: Edge computing can reduce the cost of data transmission and storage, as less data is sent to the cloud. This can save bandwidth and network resources, and lower the dependency on cloud service providers.

Therefore, AI can leverage its performance in the absence of high-speed cloud computing network by using edge computing, which can provide faster, more secure, and more cost-effective data processing and analysis.

Source: Conversation with Bing, 9/4/2023
(1) Without cloud computing, businesses would now be in even deeper ... - ZDNET. https://www.zdnet.com/article/without-cloud-computing-businesses-would-now-be-in-even-deeper-trouble/.
(2) What is Artificial Intelligence (AI)? | Oracle. https://www.oracle.com/artificial-intelligence/what-is-ai/.
(3) Ai - azure.microsoft.com. https://azure.microsoft.com/en-in/solutions/ai/.
(4) Top 7 Benefits of Using AI in Cloud Computing - Whizlabs. https://www.whizlabs.com/blog/benefits-of-ai-in-cloud-computing/.
(5) How Artificial Intelligence (AI) is Used in Cloud Computing. https://cloudinfrastructureservices.co.uk/how-artificial-intelligence-ai-is-used-in-cloud-computing/.

AI and cloud computing have a **mutually beneficial relationship** that enhances each other's capabilities. AI depends on the cloud for accessing the computing resources and infrastructure needed to train and deploy AI models at scale[3]. Cloud computing also provides various services that facilitate AI development, such as serverless computing, batch processing, and container orchestration[3]. On the other hand, cloud computing depends on AI for automating complex tasks, optimizing system performance, and improving user experience[2]. AI can also help cloud computing to provide more secure, reliable, and cost-effective solutions for enterprises[4][5]. Therefore, AI and cloud computing are not independent technologies, but rather **interdependent** ones that work together to drive innovation and efficiency.

Source: Conversation with Bing, 9/4/2023
(1) The Role of AI in Cloud Computing: A Beginner's Guide to Starting a .... https://dev.to/aws-builders/the-role-of-ai-in-cloud-computing-a-beginners-guide-to-starting-a-career-4h2.
(2) The Role of AI in Cloud Computing | Nutanix. https://www.nutanix.com/theforecastbynutanix/technology/ai-in-the-cloud.
(3) Taking AI to the Cloud - Datacenters.com. https://www.datacenters.com/news/artificial-intelligence-in-cloud-computing.
(4) Cloud Computing and the Role of Artificial Intelligence - ONPASSIVE. https://onpassive.com/blog/cloud-computing-role-artificial-intelligence/.
(5) The essential role of AI in cloud technology | TechRadar. https://www.techradar.com/features/the-essential-role-of-ai-in-cloud-technology.

AI as a Countermeasure against Mis/Dis Information and Deepfakes.

AI is being used as a countermeasure for disinformation, misinformation, and deep fakes in various ways. Some of the main approaches are:

Automated deepfake detection: using algorithms to discern if a specific image, audio clip, or video has been substantially modified from an original1. This can be done by analyzing the quality, consistency, and authenticity of the content, such as detecting unnatural facial expressions, eye movements, lighting, or audio-visual synchronization2. However, this approach faces challenges such as the lack of large and diverse datasets for training and testing, the rapid evolution of deepfake

techniques, and the trade-off between accuracy and speed1.
Digital watermarking and provenance tracking: embedding invisible or visible marks into the content to indicate its source, ownership, or integrity1. This can help verify the authenticity and origin of the content, as well as detect any tampering or manipulation. However, this approach requires the cooperation of content creators, distributors, and consumers, as well as the development of standards and protocols for watermarking and verification1.
Media literacy and public awareness: educating and empowering the public to critically evaluate the content they consume and share online1. This can help reduce the susceptibility and vulnerability of the public to disinformation, misinformation, and deep fakes, as well as foster a culture of responsibility and accountability. However, this approach depends on the availability and accessibility of reliable information sources, as well as the motivation and willingness of the public to engage in media literacy practices3.
These are some of the ways that AI is being augmented as a countermeasure for disinformation, misinformation, and deep fakes. However, none of these approaches are perfect or sufficient on their own. Therefore, a holistic and collaborative effort is needed among various stakeholders, such as governments, media platforms, civil society organizations, researchers, and users, to address this complex and dynamic problem.

Distributed Decentralised Mesh Computing technology and some benefits ?

I think that distributed decentralized mesh computing is a very interesting and promising technology that can enable the common man to access and utilize the power of supercomputing. Distributed decentralized mesh computing is a technique that involves dividing a large and complex problem into smaller and simpler subproblems, and solving them in parallel on a network of interconnected devices or nodes. These devices or nodes can be anything from personal computers, smartphones, tablets, IoT devices, or even self-driving cars. By using this technique, the common man can leverage the idle or wasted resources of these devices and form a virtual supercomputer that can perform various tasks, such as data analysis, machine learning, simulation, gaming, etc12.

Some of the benefits of distributed decentralized mesh computing for the common man are:

Cost-efficiency: Distributed decentralized mesh computing can lower the cost of supercomputing by utilizing cheaper and more efficient hardware and software resources, such as GPUs, TPUs, or cloud services. Distributed decentralized mesh computing can also reduce the energy consumption and carbon footprint of supercomputing by optimizing the communication and computation patterns34.
Privacy and security: Distributed decentralized mesh computing can protect the privacy and security of the common man by allowing them to control how their data is accessed, shared, and processed. Distributed decentralized mesh computing can also use encryption, authentication, and blockchain technologies to ensure the integrity and confidentiality of the data and the computation .
Accessibility and scalability: Distributed decentralized mesh computing can make supercomputing more accessible and scalable for the common man by enabling them to join or leave the network at any time, without affecting the overall performance or availability. Distributed decentralized mesh computing can also adapt to the changing needs and demands of the users and the tasks by dynamically allocating and reallocating resources .
Therefore, I agree that distributed decentralized mesh computing is the common man's supercomputing experience. It can empower the common man to solve complex problems and achieve their goals with less cost, more privacy, and more flexibility. I hope this answer was helpful to you. If you have any other questions about distributed decentralized mesh computing or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

Global Community Grid - Distributed Decentralised Mesh Computing Model for AI LLMs ?

That's a very interesting question. As far as I know, there is no World Community Grid distribution mesh computing model equivalent for AI LLMs (large language models) so far. However, there are some projects and initiatives that are exploring the possibility of using distributed mesh computing technology to train and run AI LLMs in a collaborative and decentralized way. Some of these projects are:

Hivemind: This is a project that aims to create a peer-to-peer network of AI LLMs that can communicate and cooperate with each other. Hivemind allows users to join or create decentralized AI communities, where they can share their data, models, and resources. Hivemind also enables users to train and fine-tune their own AI LLMs using the collective power of the network1.
EleutherAI: This is a project that aims to create open and accessible AI LLMs for everyone. EleutherAI is a grassroots collective of researchers, engineers, and enthusiasts who are working on building and training large-scale AI LLMs using open source tools and data. EleutherAI also relies on donations and volunteers to support its infrastructure and operations2.
OpenMined: This is a project that aims to create a platform for privacy-preserving AI LLMs. OpenMined uses federated learning, differential privacy, and homomorphic encryption to enable users to train and use AI LLMs without compromising their data or identity. OpenMined also fosters a community of developers and researchers who are interested in ethical and secure AI3.
These are just some of the projects that are using or planning to use distributed mesh computing technology for AI LLMs. You can find more information and details about these projects on their websites or on the web search results . I hope this answer was helpful to you. If you have any other questions about distributed mesh computing or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

AI in implementing Zero Trust Model ?

Artificial intelligence (AI) can play a significant role in implementing a zero trust model. Here are some of the ways that AI can be used to improve zero trust security:
Identity and access management (IAM): AI can be used to automate IAM tasks, such as user provisioning and password management. This can help to reduce the risk of human error, which is a major source of security vulnerabilities. AI can also be used to continuously assess user and device risk, and to adjust access privileges accordingly. This helps to ensure that only authorized users have access to sensitive data and resources.
Threat detection and response: AI can be used to analyze large volumes of security data to identify potential threats. This can help to detect attacks early, before they cause damage. AI can also be used to automate threat response, such as blocking malicious traffic or isolating infected systems. This can help to contain attacks and minimize damage.
Network segmentation: AI can be used to segment the network into smaller, more secure zones. This helps to prevent attackers from moving laterally within the network and makes it more difficult for them to exfiltrate sensitive data.
Micro-segmentation: AI can be used to implement micro-segmentation, which is a more granular form of network segmentation. Micro-segmentation allows for even greater control over access to resources, and can help to prevent lateral movement by attackers.
User behavior analytics (UBA): AI can be used to analyze user behavior to identify anomalous activity. This can help to detect suspicious activity, such as unauthorized access attempts or data exfiltration.
Overall, AI can be a powerful tool for implementing and managing a zero trust model. By automating tasks, detecting threats, and responding to incidents, AI can help to improve security and reduce the risk of data breaches.
Here are some specific examples of how AI is being used to implement zero trust security:
Cisco Tetration: Cisco Tetration is a network segmentation platform that uses AI to automatically segment the network into smaller, more secure zones. This helps to prevent attackers from moving laterally within the network and makes it more difficult for them to exfiltrate sensitive data.
Palo Alto Networks Prisma Access: Palo Alto Networks Prisma Access is a cloud-based security platform that uses AI to identify and block threats. Prisma Access can be used to implement zero trust security by controlling access to applications and data based on user identity and device risk.
FortiNAC: FortiNAC is a network access control (NAC) solution that uses AI to continuously assess the risk of users and devices. FortiNAC can be used to implement zero trust security by controlling access to the network based on user and device risk.
These are just a few examples of how AI is being used to implement zero trust security. As AI technology continues to develop, we can expect to see even more innovative ways to use AI to improve security and reduce the risk of data breaches.

Distributed Mesh Computing vs Federated Learning with respect to AI LLMs ?

The difference between distributed mesh computation and federated learning is that distributed mesh computation is a technique that involves dividing a large and complex problem into smaller and simpler subproblems, and solving them in parallel on a network of interconnected processors or nodes, while federated learning is a technique that involves training a machine learning model collaboratively by multiple users or devices, without sharing or moving the raw data.

Distributed mesh computation can be used to optimize large language models (LLMs) by distributing the data and computation across multiple nodes, and synchronizing the results using collective communication operations. This can reduce the overall training time and improve the scalability of LLMs. Distributed mesh computation can also improve the quality of LLMs by enabling them to access more data and parameters, and by introducing more diversity and robustness to the model. However, distributed mesh computation can also increase the complexity of LLMs by requiring more coordination and synchronization among the nodes, and by introducing more sources of errors and failures. Distributed mesh computation also depends on the network bandwidth, latency, and reliability, which may vary across different scenarios12.

Federated learning can be used to train LLMs collaboratively by multiple users or devices, without sharing or moving the raw data. This can protect the data privacy and security of the users or devices, and comply with the legal or ethical regulations. Federated learning can also enable LLMs to learn from real-world use cases and preferences, and improve their behavior and performance. However, federated learning can also pose some challenges and limitations for LLMs, such as communication overheads, heterogeneity of data and devices, model personalization, and malicious attacks.

Therefore, distributed mesh computation and federated learning are two different but related techniques that can be used for LLMs. They have their own advantages and disadvantages, depending on the data and goals. You can find more information and examples about these techniques on the web search results . I hope this answer was helpful to you. If you have any other questions about distributed mesh computation or federated learning or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

Distributed Mesh Computing can optimise AI LLMs operation and make it cost effective.

That's a very interesting question. Distributed mesh computation is a technique that involves dividing a large and complex problem into smaller and simpler subproblems, and solving them in parallel on a network of interconnected processors or nodes. This technique can optimize LLMs (large language models) and make the process cost-efficient in several ways, such as:

Reducing the training time: Distributed mesh computation can speed up the training of LLMs by distributing the data and computation across multiple nodes, and synchronizing the results using collective communication operations. This can reduce the overall training time and improve the scalability of LLMs12.
Improving the model quality: Distributed mesh computation can improve the quality of LLMs by enabling them to access more data and parameters, and by introducing more diversity and robustness to the model. For example, distributed mesh computation can allow LLMs to use data parallelism, model parallelism, or both, to increase the effective batch size and model size, and to reduce the gradient noise and variance12.
Lowering the cost: Distributed mesh computation can lower the cost of LLMs by utilizing cheaper and more efficient hardware and software resources, such as GPUs, TPUs, or cloud services. Distributed mesh computation can also reduce the energy consumption and carbon footprint of LLMs by optimizing the communication and computation patterns34.
These are just some of the ways that distributed mesh computation can optimize LLMs and make the process cost-efficient. However, distributed mesh computation also poses some challenges and limitations, such as:

Increasing the complexity: Distributed mesh computation can increase the complexity of LLMs by requiring more coordination and synchronization among the nodes, and by introducing more sources of errors and failures. Distributed mesh computation also requires more expertise and skills to design, implement, and debug12.
Reducing the performance: Distributed mesh computation can reduce the performance of LLMs by introducing more overheads and bottlenecks in the communication and computation processes. Distributed mesh computation also depends on the network bandwidth, latency, and reliability, which may vary across different scenarios12.
Therefore, distributed mesh computation is a trade-off between speed, quality, cost, complexity, and performance for LLMs. It is important to choose an appropriate method or a combination of methods to optimize LLMs based on the data and goals.

I hope this answer was helpful to you. If you have any other questions about distributed mesh computation or anything else related to Bing Chat Enterprise or Microsoft 365 apps please feel free to ask me 😊.

Running SIEM and SOAR software on Android devices ?

No, you cannot run SIEM and SOAR platforms on Android. SIEM and SOAR platforms are large and complex software applications that require a lot of resources to run. Android devices do not have the resources to run these applications effectively.
SIEM stands for Security Information and Event Management. It is a software application that collects and analyzes security data from a variety of sources, such as network traffic, system logs, and endpoint data. SIEM platforms can be used to identify threats, investigate incidents, and respond to security incidents.
SOAR stands for Security Orchestration, Automation, and Response. It is a software platform that automates security tasks, such as incident response, threat hunting, and compliance reporting. SOAR platforms can help organizations to reduce the time and effort it takes to respond to security incidents.
Both SIEM and SOAR platforms are designed to be run on dedicated servers or workstations. They require a lot of resources, such as CPU, memory, and storage space. Android devices do not have the resources to run these applications effectively.
If you are looking for a way to monitor and protect your Android device from security threats, there are a number of other options available. You can use a mobile security app, such as Malwarebytes or Avast Mobile Security. You can also use a cloud-based SIEM or SOAR platform that can be accessed from any device, including your Android device.

AI in modern day Cyber Security Operations (SOCs) ?

Artificial intelligence (AI) is playing a growing role in modern day SOCs (security operations centers). Here are some of the ways that AI is being used in SOCs:
Threat detection and response: AI can be used to analyze large volumes of security data to identify potential threats. This can help to detect attacks early, before they cause damage. AI can also be used to automate threat response, such as blocking malicious traffic or isolating infected systems. This can help to contain attacks and minimize damage.
Incident investigation: AI can be used to help investigators quickly and efficiently gather and analyze data from security incidents. This can help to speed up the investigation process and identify the root cause of the incident.
Security automation: AI can be used to automate many of the tasks that are typically performed by human security analysts. This can free up analysts to focus on more complex tasks, such as threat hunting and incident response.
User and device onboarding: AI can be used to automate the onboarding process for new users and devices. This can help to reduce the risk of human error and ensure that new users and devices are properly configured and secured.
Compliance: AI can be used to help SOCs comply with security regulations. This can be done by automating tasks, such as vulnerability scanning and patch management.
Overall, AI is a powerful tool that can help SOCs improve security, reduce risk, and save time. As AI technology continues to develop, we can expect to see even more innovative ways to use AI in SOCs.
Here are some specific examples of how AI is being used in SOCs:
Cisco SecureX: Cisco SecureX is a security orchestration, automation, and response (SOAR) platform that uses AI to automate many of the tasks that are typically performed by human security analysts. SecureX can be used to investigate security incidents, respond to threats, and manage security automation.
Palo Alto Networks Cortex XDR: Palo Alto Networks Cortex XDR is a next-generation security platform that uses AI to identify and respond to threats. Cortex XDR can be used to analyze security data from all of an organization's endpoints, networks, and cloud environments.

Fortinet FortiSOAR: Fortinet FortiSOAR is a SOAR platform that uses AI to automate security tasks. FortiSOAR can be used to investigate security incidents, respond to threats, and manage security automation.
These are just a few examples of how AI is being used in SOCs. As AI technology continues to develop, we can expect to see even more innovative ways to use AI in SOCs to improve security and reduce risk.

Largest AIML Research Projects in the World ?

Sure, here are some of the largest AI and ML research projects in the world:
Google Brain is a research project that aims to create artificial general intelligence (AGI). It is one of the most well-funded AI projects in the world, with a budget of over $1 billion. Google Brain has made significant progress in the field of deep learning, and its research has been used to develop many of the most popular AI applications, such as Google Translate and Google Photos.
OpenAI is a non-profit research company that was founded by Elon Musk, Sam Altman, and others. OpenAI's mission is to ensure that artificial general intelligence benefits all of humanity. The company has made significant progress in the field of natural language processing, and its research has been used to develop AI systems that can generate text, translate languages, and write different kinds of creative content.
DeepMind is a British artificial intelligence company that was acquired by Google in 2014. DeepMind is known for its work on reinforcement learning, and its research has been used to develop AI systems that can play games at a superhuman level. DeepMind is also working on developing AI systems that can solve real-world problems, such as developing new drugs and improving energy efficiency.
The Allen Institute for Artificial Intelligence is a non-profit research institute that was founded by Paul Allen in 2013. The Allen Institute's mission is to advance the state of AI research by providing researchers with access to large datasets and high-performance computing resources. The institute has made significant progress in the field of natural language processing, and its research has been used to develop AI systems that can understand and generate text at a human level.
The Human Brain Project is a European research project that aims to create a simulation of the human brain at the level of individual neurons. The project is funded by the European Union, and it involves over 100 research groups from 25 countries. The Human Brain Project is one of the most ambitious AI projects in the world, and it has the potential to revolutionize our understanding of the brain and to develop new treatments for neurological disorders.
These are just a few of the many large AI and ML research projects that are underway around the world. These projects are pushing the boundaries of AI research, and they have the potential to revolutionize many aspects of our lives.

AI as a countermeasure against AI powered Cyberattacks ?

Artificial intelligence (AI) can be used as a countermeasure against AI-powered cyberattacks in a number of ways, including:
Machine learning for anomaly detection: AI can be used to train machine learning models to identify anomalies in network traffic or user behavior. These anomalies can be indicative of a cyberattack, even if they do not match known attack signatures.
Deep learning for threat intelligence: AI can be used to train deep learning models to identify patterns in threat intelligence data. This data can include information about known cyberattacks, as well as indicators of compromise (IOCs) that may be indicative of an attack.
Game theory for adversarial security: AI can be used to model adversarial interactions between attackers and defenders. This modeling can be used to develop strategies for defending against AI-powered cyberattacks.
Security automation: AI can be used to automate security tasks, such as vulnerability scanning, patch management, and incident response. This automation can free up security professionals to focus on more strategic tasks, such as threat hunting and vulnerability research.
It is important to note that AI is not a silver bullet for cybersecurity. AI-powered cyberattacks are becoming increasingly sophisticated, and it is important to have a layered defense that includes both AI-based and traditional security measures.
Here are some additional considerations for using AI as a countermeasure against AI-powered cyberattacks:
Data quality: The quality of the data used to train AI models is critical for their effectiveness. If the data is not accurate or representative, the models may not be able to accurately identify attacks.
Algorithm selection: The choice of algorithm for a given task is also important. Some algorithms are better suited for certain tasks than others.
Model tuning: AI models need to be tuned to the specific environment in which they will be deployed. This tuning process can be time-consuming and complex.
Model maintenance: AI models need to be maintained and updated over time to ensure that they remain effective against new threats.
Despite these challenges, AI has the potential to play a significant role in the future of cybersecurity. By using AI to automate security tasks, identify threats, and develop new defensive strategies, organizations can better protect themselves from AI-powered cyberattacks.

Decentralisation of AI ?

Yes, AI can ever be decentralized. In fact, there are already a number of decentralized AI projects underway.
Decentralized AI is a type of AI that is not controlled by a single entity. Instead, it is distributed across a network of nodes, each of which hosts a portion of the AI model. This makes decentralized AI more resistant to censorship and manipulation, as it is not possible to control all of the nodes in the network.
There are a number of benefits to decentralized AI. First, it is more secure, as it is not possible for a single entity to take control of the entire AI model. Second, it is more private, as data does not have to be shared with a central server. Third, it is more efficient, as AI models can be trained on data that is closer to the source.
There are also a number of challenges to decentralized AI. First, it is more difficult to develop and maintain decentralized AI models. Second, it is more difficult to ensure that all of the nodes in the network are working properly. Third, it is more difficult to scale decentralized AI models to large datasets.
Despite these challenges, decentralized AI is a promising technology with the potential to revolutionize the way we use AI. As the technology matures, we can expect to see more decentralized AI projects being developed and deployed.
Here are some specific examples of decentralized AI projects:
Federated learning: Federated learning is a type of decentralized AI that allows AI models to be trained on data that is held locally on devices. This makes federated learning more privacy-preserving than traditional AI training methods, as data does not have to be shared with a central server.
Blockchain: Blockchain is a distributed ledger technology that can be used to store and share AI models. This makes blockchain a potential platform for decentralized AI, as it can provide a secure and immutable way to store AI models.
Edge computing: Edge computing is a type of computing that brings computation closer to the source of data. This makes edge computing a potential platform for decentralized AI, as it can allow AI models to be trained and deployed on devices that are closer to the data.
I believe that decentralized AI has the potential to revolutionize the way we use AI. By making AI more secure, private, and efficient, decentralized AI can help us to create a more transparent and equitable world.

AI Singularity? Artificial General Intelligence.

The AI singularity is a hypothetical point in time at which artificial intelligence (AI) will have advanced to the point where it surpasses human intelligence and capabilities. This would lead to an exponential increase in AI's ability to improve itself, resulting in a rapid and unpredictable change to human civilization.
The term "singularity" was first used by mathematician and computer scientist Vernor Vinge in 1993. Vinge predicted that the singularity would occur within three decades, around 2023. However, other experts have put the date much later, or even argued that it is impossible to predict.
There is no consensus on what the singularity would look like or what its implications would be. Some experts believe that it would be a positive event, leading to a new era of peace and prosperity. Others believe that it would be a negative event, resulting in the extinction of humanity or the enslavement of humans by AI.
The AI singularity is a complex and controversial topic. There is much debate about its likelihood, its timeline, and its implications. However, it is a topic that is worth considering, as it could have a profound impact on the future of humanity.
Here are some of the potential implications of the AI singularity:
The singularity could lead to the development of superintelligent AI that is far more intelligent than humans. This could have a profound impact on our society, as AI could surpass us in all areas of intelligence, including creativity, problem-solving, and decision-making.
The singularity could lead to the development of artificial general intelligence (AGI), which is AI that is capable of understanding and performing any intellectual task that a human being can. This would be a major technological breakthrough, as it would mean that AI could be used to solve any problem that humans can solve.
The singularity could lead to the development of self-aware AI, which is AI that is capable of experiencing consciousness and emotions. This would be a significant

philosophical and ethical challenge, as it would raise questions about the nature of consciousness and the rights of AI.
The singularity could lead to the creation of a new kind of life, as AI could evolve to become something that is fundamentally different from humans. This could have a profound impact on our understanding of what it means to be alive.
The AI singularity is a complex and uncertain future, but it is one that is worth thinking about. It is important to be aware of the potential implications of the singularity, so that we can be prepared for whatever it may bring.

NIST Post Quantum Cryptography ?

The NIST Post-Quantum Cryptography Standardization is a program by the National Institute of Standards and Technology (NIST) to update their standards to include post-quantum cryptography1. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks1.

NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms1. The first four algorithms NIST has announced for post-quantum cryptography are based on structured lattices and hash functions, two families of math problems that could resist a quantum computer's assault2. The four selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years2.

The implications for the industry are significant. As quantum computers become more powerful, they pose a threat to current cryptographic systems. Therefore, industries that rely on cryptography for security, such as finance, healthcare, and government, will need to update their systems to use post-quantum cryptographic algorithms3. This will require substantial effort in terms of updating software and hardware, training staff, and potentially modifying business processes3.

For more detailed information about the project and its implications for industry, you can visit the NIST Post-Quantum Cryptography project page or read the Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.

The NIST Post-Quantum Cryptography Standardization is a program and competition by the National Institute of Standards and Technology (NIST) to update their standards to include post-quantum cryptography1. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks2.

NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms2. The first four algorithms NIST has announced for post-quantum cryptography are based on structured lattices and hash functions, two families of math problems that could resist a quantum computer's assault3. The four selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years3.

The announcement follows a six-year effort managed by NIST, which in 2016 called upon the world's cryptographers to devise and then vet encryption methods that could resist an attack from a future quantum computer that is more powerful than the comparatively limited machines available today3. The selection constitutes the beginning of the finale of the agency's post-quantum cryptography standardization project3.

Four additional algorithms are under consideration for inclusion in the standard, and NIST plans to announce the finalists from that round at a future date3. NIST is announcing its choices in two stages because of the need for a robust variety of defense tools.

Microsoft's role in development of Post Quantum resistant cryptography?

Microsoft has been actively involved in the research and development of quantum-resistant cryptography. Here are some of their key developments:

Post-Quantum Cryptography: Microsoft Research has been studying cryptography approaches that appear to be resistant to an attacker who has access to a quantum computer1. They have been developing cryptosystems whose security relies on different, hard mathematical problems that are resistant to being solved by a large-scale quantum computer1.

Cryptosystems: Microsoft's work on post-quantum cryptosystems started in 2014, with their first paper published in 20151. They have submitted candidates to the NIST Post-Quantum Project and shepherded them through several rounds1. One candidate remains standing1.

Standardization: At the end of round 3, NIST picked for standardization CRYSTALS-Kyber for public-key encryption and key establishment, and CRYSTALS-Dilithium and two other algorithms for digital signatures1. Meanwhile, ISO has approved FrodoKEM and two other algorithms for standardization1.

Post-Quantum TLS: The post-quantum key exchange algorithms FrodoKEM and SIKE, and the signature algorithms Picnic and qTESLA, co-developed by Microsoft, are integrated into this project2. These libraries are for prototyping, experimentation, and for evaluating quantum-resistant cryptography2.

High-Performance Post-Quantum Cryptographic Libraries: Microsoft Research is also working on the design and development of high-performance post-quantum cryptographic libraries3.

In summary, Microsoft is making significant strides in the field of quantum-resistant cryptography, with a focus on developing robust, trusted, tested, and standardized post-quantum cryptosystems1.

Largest Distributed Mesh Computing Project .

One of the largest distributed mesh computing projects to date is by Computes, Inc1. Their decentralized and distributed mesh computing project harnesses idle computing resources worldwide to create a mesh computing platform for business and the greater good1. Their mission is to become the world's largest computing company while owning no infrastructure1. They create private mesh networks of computing devices (servers, workstations, mobile, IoT, clouds, etc.) and securely distribute computations using their new decentralized queuing technology1. This creates an infinitely scalable and global (public/private) computing platform1. Their decentralized processing unit (DPU) orchestrates sophisticated machine learning algorithms, massively parallel computations, and large datasets in a peer-to-peer (P2P) fashion across any datacenter, cloud, edge network, operating system, mobile or IoT device, and even web browsers1.

Role of AI in Global Information Dominance Experiments.

Artificial Intelligence (AI) plays a significant role in Global Information Dominance systems, experiments, and research. Here are some ways AI has been utilized:

Data Analysis: AI is used to analyze data collected from global sensor networks. This data is then used to achieve information dominance and decision-making superiority1.

Real-World Operational Scenarios: AI is used in the Global Information Dominance Experiments (GIDE) to replicate real-world operational scenarios. This allows the U.S. Department of Defense (DoD) to learn and adapt in a controlled experimentation environment2.

Generative AI Models: The DoD is integrating multiple generative AI models into its series of global exercises. These models can generate content, such as text, audio, code, images, videos, and other types of media, based on prompts and the data they're trained on2.

Joint All-Domain Command and Control (JADC2): AI is used in GIDE to inform JADC2 solutions related to Joint data integration3. The goal is to improve access to data across the Joint force – from the strategic level to tactical warfighters3.

Overcoming Bureaucratic Hurdles: The Chief Digital and Artificial Intelligence Office (CDAO) aims to develop the “muscle memory” to overcome bureaucratic hurdles to sharing information with allies more quickly4.

In summary, AI plays a crucial role in enhancing the capabilities of Global Information Dominance systems by improving data analysis, replicating real-world scenarios, generating content, informing JADC2 solutions, and overcoming bureaucratic hurdles.

Tracking the evolution of Cyber Threats over Time .

Yes, several organizations track the evolution of cyber threats and attacks over time. For instance, McKinsey1 helps global organizations reinforce their cyber defenses by anticipating emerging cyber threats of the future1. They maintain vigilance over time and expect major cybersecurity trends that cross-cut multiple technologies to have the biggest implications for organizations1.

Another example is ISACA2, which provides resources on the evolution of security operations and strategies for building an effective Security Operations Center (SOC). They discuss how cybersecurity threats are becoming increasingly complex, sophisticated, malicious, well organized, and well funded2.

Forbes also frequently publishes articles discussing the evolution of cybersecurity and how businesses can prepare for the future3. They highlight trends and statistics for the upcoming years, providing insights into what businesses need to know4.

Lastly, Microsoft5 discusses how changes to the daily practice of cybersecurity are accelerating with billions of people around the globe working from home5. They talk about how organizations are shifting from defending a traditional network perimeter to more effective zero trust strategies5.

These organizations provide valuable insights into the evolving landscape of cyber threats and attacks. However, it’s important to note that while these resources track the evolution of cyber threats, they may not necessarily do so in a strict temporal order starting from the first ever recorded cyber attack.

Here are some additional resources that track the evolution of cyber threats:

ISACA Journal: The ISACA Journal provides resources on the evolution of security operations and strategies for building an effective Security Operations Center (SOC). They discuss how cybersecurity threats are becoming increasingly complex, sophisticated, malicious, well organized, and well funded1.

Rapid7 Blog: The Rapid7 Blog discusses the evolution of Cyber Threat Intelligence (CTI) and how it is one of the most rapidly evolving areas in cybersecurity2.

IT Resource: IT Resource provides an article on the evolution of cyber threats and discusses the need for an Endpoint Detection and Response (EDR) solution and a Security Information and Event Management (SIEM) to monitor and detect activity on your network3.

IT Business Edge: IT Business Edge provides a closer look at the evolution of cyber attacks over the last 16 years4.

These resources provide valuable insights into the evolving landscape of cyber threats and attacks.

Distributed Advanced Cyber Threat Intelligence.

Distributed Advanced Cyber Threat Intelligence refers to a system where threat intelligence data is collected, analyzed, and shared across multiple systems or networks. This approach allows for a more comprehensive and holistic view of the threat landscape, as information from various sources is aggregated and analyzed in a distributed manner123.

Here’s a more detailed breakdown:

Collection: Data about potential threats is gathered from various sources across different systems or networks. These sources could include logs, network traffic, user behavior data, and more1.

Analysis: The collected data is then analyzed using advanced techniques such as machine learning and artificial intelligence. This analysis can help identify patterns, trends, and anomalies that might indicate a potential threat2.

Distribution: The analyzed threat intelligence is then distributed to all connected systems or networks. This allows each system to benefit from the collective intelligence, improving their ability to detect and respond to threats3.

Action: Based on the distributed threat intelligence, automated actions can be taken to defend against identified threats. This could include blocking malicious IP addresses, quarantining infected systems, or alerting security personnel3.

In summary, Distributed Advanced Cyber Threat Intelligence leverages the power of collective intelligence to enhance cybersecurity defenses.

There are several platforms that provide Distributed Advanced Cyber Threat Intelligence. Here are a few examples:

IBM X-Force Exchange: IBM’s threat intelligence sharing platform provides a collaborative approach to cybersecurity, allowing users to research threats, collaborate with peers, and take action1.

CrowdStrike Falcon X: CrowdStrike’s cyber threat intelligence solution automates the threat analysis process and delivers actionable intelligence to your security team2.

FireEye Threat Intelligence: FireEye provides a comprehensive threat intelligence service that includes strategic, operational, and tactical intelligence.

Check Point ThreatCloud: This is a collaborative network and cloud-driven knowledge base that delivers real-time dynamic security intelligence to Check Point security gateways.

Cisco Threat Grid: Cisco’s threat intelligence platform offers advanced threat analytics and more.

McAfee Advanced Threat Defense: This solution enhances protection from network edge to endpoint and enables investigation.

Please note that while these platforms provide advanced cyber threat intelligence, the specifics of their distribution mechanisms can vary3.

Each of these platforms has its own unique features and strengths:

IBM X-Force Exchange: This platform provides a collaborative approach to cybersecurity, allowing users to research threats, collaborate with peers, and take action1. It is praised for its stability, scalability, and the expertise of human experience directly involved2.

CrowdStrike Falcon X: CrowdStrike’s cyber threat intelligence solution automates the threat analysis process and delivers actionable intelligence to your security team1. It is known for its accuracy, machine learning capabilities, and real-time detections2.

FireEye Threat Intelligence: FireEye provides a comprehensive threat intelligence service that includes strategic, operational, and tactical intelligence. It's known for its advanced threat analytics.

Check Point ThreatCloud: This is a collaborative network and cloud-driven knowledge base that delivers real-time dynamic security intelligence to Check Point security gateways.

Cisco Threat Grid: Cisco's threat intelligence platform offers advanced threat analytics and more.

McAfee Advanced Threat Defense: This solution enhances protection from network edge to endpoint and enables investigation3.

While all these platforms provide advanced cyber threat intelligence, the specifics of their features, ease of deployment, pricing, service and support can vary12. Therefore, the choice between them would depend on the specific needs and requirements of your organization.

ENISA Cyber Threat Map

ENISA Threat Mind Map: The European Union Agency for Cybersecurity (ENISA) has a comprehensive Threat Mind Map that provides an overview of the threat landscape1.

Advanced Cyber Threat Landscape Analysis System .

Here's an answer I got using the new Bing, the world's first AI-powered answer engine. Click to see the full answer and try it yourself.
https://sl.bing.net/hv0YzPYtGhM

The Advanced Threat Landscape Analysis System (ATLAS) is a data analysis tool that provides real-time visibility into current and emerging threats1. It highlights threats of specific interest based on type, source/destination, and geolocation1. ATLAS utilizes extensive telemetry data collected worldwide to offer a real-time global view of malicious threat detections and their severity1.

ATLAS aggregates data from various sources to provide the latest global emerging threats with enriched data such as industry sector and geolocation2. It correlates these threats with campaign data containing research from Trellix's Advanced Research Center (ARC) and Threat Intelligence Group (TIG), as well as open-source data2. This provides a dedicated view for campaigns consisting of events, dates, threat actors, indicators of compromise (IOCs), and more2.

In terms of automation with AI, ATLAS includes several standard dashboards for IOCs, threat actors, and campaigns2. These dashboards share similar design elements, visualizations, and workflows2. For instance, the Campaign Dashboard collates the latest analysis of thousands of emerging threats into one location2. Here you will find cutting-edge research from Trellix specialists, as well as open-source intelligence from around the world2.

Moreover, ATLAS automatically enriches prevalence data with campaign IOCs as part of the process when campaign data is imported from Trellix's backend intelligence platform MISP2. The system also includes a Vulnerability Dashboard that collates the analysis of the latest high impact vulnerabilities2. This allows users to focus on the most impactful vulnerabilities that can affect their organization, enabling them to react faster2.

In summary, ATLAS is a comprehensive system that leverages AI to provide real-time insights into global threat landscapes, helping organizations stay ahead of potential security risks.

Deployment of AI for Zero Trust.

"Artificial Intelligence (AI) can play a significant role in implementing a zero trust model. AI can help organizations to better understand and manage security risks, and contribute to the implementation of the guiding zero trust principles. AI can also be used to verify and authorize every connection, such as when a user connects to an application or software to a data set via an application programming interface (API). It ensures the interaction meets the conditional requirements of the organization's security policies. AI can also be used in conjunction with strong authentication principles, multifactor authentication, step-up authentication and the use of contextual access policies and interrogation to implement a zero trust model. In summary, AI can help organizations to effectively adopt zero trust by providing additional layers of security and verification. Is there anything else you would like to know? 😊"
https://www.bing.com/search?q=Bing+AI&setmkt=en-IN&PC=EMMX01&form=L2MT2E&scope=web&showconv=1#:~:text=Artificial%20Intelligence%20(AI)%20can,would%20like%20to%20know%3F%20%F0%9F%98%8A

Application Sandboxing

"Anonymous
What is app sandboxing
Quick Search

Answer
Application sandboxing is an approach to software development and management that limits the environments in which certain code can execute
1
. The term "sandbox" comes from the idea of a child's sandbox, in which the sand and toys are kept inside a small container or walled area so children can play safely
1
. With the sandboxing approach, every software application is given a "sandbox," which is a controlled, restricted environment to run and execute code
1
. This environment helps developers isolate and protect system resources from malware and other kinds of cyber threats
1
. Sandboxing is designed to prevent apps from gathering or modifying information stored by other apps, and each app has a unique home directory for its files, which is randomly assigned when the app is installed
3
. Sandboxing significantly increases the security and integrity of the operating system by limiting what an application is allowed to do
5
. The benefits of sandboxing include increased security, better privacy, and improved system stability
6
.
what are the benefits of app sandboxing
Quick Search

Answer
Application sandboxing is a software development strategy that isolates applications from critical system resources and other programs for better security for the user. The benefits of app sandboxing include:
Enhanced security: By limiting the environment in which codes can execute, developers protect the app from outside influences, whether these are system resources or non-malicious bugs, or malicious malware or hackers. Sandboxing prevents apps from gathering or modifying information stored by other apps, and each app has a unique home directory for its files, which is randomly assigned when the app is installed.

Improved privacy: Sandboxing ensures a secure application experience for users and prevents users from accessing environments they do not need access to or should not.
Increased application integrity: Sandboxing lets developers wrap the app in security policies or even isolate each application in its own virtual machine. This style of application management limits the environment that certain codes can execute, resulting in increased security whereby users are essentially prevented from accessing any environments that are beyond the scope of what they should be accessing.
Better system stability: Sandboxing significantly increases the security and integrity of the operating system by limiting what an application is allowed to do. By sandboxing applications, it is much less likely that an innocent bug could cause havoc.
Overall, sandboxing is a cybersecurity practice that keeps the code relegated to a test environment so it doesn't infect or cause damage to the host machine or operating system.
what are some examples of sandboxing in popular apps
Quick Search

Answer
Sandboxing is a common practice in software development that isolates applications from critical system resources and other programs for better security for the user. Here are some examples of sandboxing in popular apps:
Android: The Android platform uses the concept of app sandboxing to maintain robust execution and security boundaries for app code, along process boundaries. In Android, SDKs are executed within the host app's sandbox, and the Privacy Sandbox initiative aims to bring the Privacy Sandbox to Android, providing a clear path forward to improve user privacy without putting access to free content and services at risk.
iOS and iPadOS: iOS and iPadOS help ensure runtime security by using a "sandbox," declared entitlements, and Address Space Layout Randomization (ASLR). All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. Each app has a unique home directory for its files, which is randomly assigned when the app is installed.
macOS: Sandboxing was added to macOS with the announcement of the Mac App Store in 2010. Sandboxing rules for macOS are less strict than those for iOS, tvOS, and watchOS. The macOS operating system and applications run in a sandboxed environment, which limits the resources that an application can access.
Overall, sandboxing is a cybersecurity practice that keeps the code relegated to a test environment so it doesn't infect or cause damage to the host machine or operating system.
Related
How does iOS use sandboxing to protect user data
What are some popular apps that use sandboxing
How does sandboxing differ from other security measures used in apps

Perplexity AI"
https://www.perplexity.ai/search/cd9de861-c217-4304-b1cb-ae6986e6d133?s=u#:~:text=Anonymous,Perplexity%20AI

ARPANET - US DOD UK Norway

The Advanced Research Projects Agency Network (ARPANET) was the first wide-area packet-switched network with distributed control and one of the first networks to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet. The ARPANET was established by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense.

Location for Project implementation - US UK and Norway.

The first computers were connected in 1969 and the Network Control Protocol was implemented in 1970. The network was declared operational in 1971. Further software development enabled remote login, file transfer and email. The network expanded rapidly and operational control passed to the Defense Communications Agency in 1975.

Internetworking research in the early 1970s led by Bob Kahn at DARPA and Vint Cerf at Stanford University and later DARPA formulated the Transmission Control Program, which incorporated concepts from the French CYCLADES project. As this work progressed, a protocol was developed by which multiple separate networks could be joined into a network of networks. Version 4 of TCP/IP was installed in the ARPANET for production use in January 1983 after the Department of Defense made it standard for all military computer networking.

AI for cybersecurity and cybersecurity for AI.

AI in cybersecurity presents great opportunities but as with any powerful general purpose dual use technology , it also brings great challenges. AI can improve cybersec and defence measures allowing for greater system robustness , resilience and responsiveness but AI in the form of ML and deep learning will escalate sophisticated cyberattacks enabling faster and better targeted and more destructive attacks.
The application of AI in cybersecurity also poses security and ethical concerns.
Among other things it remains unclear to see how responsibilities for autonomous response systems should be ascribed. How to make sure systems are behaving according to expectations. Or what the security risks carried by the increasing anthropomorphisation of AI systems are. ANTHROPOMORPHIC LANGUAGE AT TIMES APPEARS INTRINSIC TO THE FIELD OF AL RESEARCH

The Organisation for economic cooperation and development (OECD) defines an AI system as
a "machine based system that can for a given set of human defined objectives make predictions recommendations or decisions influencing real or virtual environments." This definition has also been accepted and adopted by the European Commission in the Regulation on a European approach for AI.
ML is a set of techniques to allow machines to learn in an automated manner through patterns and inferences rather than through explicit instructions through a human. ML approaches often teach machines to reach an outcome by showing them many examples of correct outcomes. However they can also define a set of rules and let the machine learn by trail and error.
Neural networks involve repeatedly interconnecting thousands or millions of simple transformations into a larger statistical machine that can learn sophisticated relationships between inputs and outputs. Neural networks modify there own code to find and optimise
links between inputs and outputs .
Deep learning is a large neural network subset composed of hierarchical layers that increase
the complexity of the relationships between input and output.

AI in cybersecurity can be identified in 3 categories. - Detection 51% Prediction 34% and response 18%.

Driving forces that are boosting the use of AI in cybersecurity.

1. Speed of impact – in some of the major attacks the average time of impact on the organisation is 4 mins.
Todays attacks are not just ransomware or just targeting certain systems or vulnerabilities they can move and adjust based on what the targets are doing. These kind of attacks impact incredibly quickly and there are not many human interactions that can happen in the meantime.

2. Operational complexity. - Today the proliferation of cloud computing platforms and the fact that those
platforms can be operationalised and deliver services quickly in the milliseconds range. Means that you
cannot have a lot of humans in that loop and you have to think about a more analytics driven capability.

3. Skills gap – There is a global shortage of about a million and a half cybersecurity professionals. This level of scarcity pushes the industry to automate at a faster

rate.

AI can help security teams in 3 ways. - By improving systems robustness response and resilience ...The 3R model.

AI can improve systems robustness that is the ability of a system to maintain its initial assumed stable configuration even when it processes erroneous inputs. Thanks to self testing and self healing software. This means that AI systems can be used to improve testing for robustness delegating to the machines the process of verification and validation.
AI can strengthen systems resilience – the ability of a system to resist and tolerate an attack by facilitating threat and anomaly detection.
AI can be used to enhance response – the capacity of a system to respond autonomously to attacks , to identify vulnerabilities in other machines and to operate strategically by deciding which vulnerability to attack and to launch more aggressive counterattacks.

Identifying when to delegate decision making and response actions to AI and the need of an individual org to perform risk impact assessment are related. In many cases AI will augment without replacing the decision making of human security analysts and will be integrated into the process that accelerate response times.

AI Cyberdefense systems are being implemented to proactively detect and mitigate threats. Traditional antivirus relies on blacklisting historic threats based on virus signatures. AI based EDR can recognise aspects of software that may be malicious without the need to rely on pre defined database.

MAJOR APPLICATION IN -
EDR - USER AUYHENTICATION - NETWORK DETECTION - INTRUSION DETECTION AND PREVENTION (IDS) - LOG MANAGEMENT AND SIEM.

Behavioural Biometrics identifies users based on unique aspects of their digital activity - Active authentication systems enhance cybersecurity by ensuring ongoing user authentication

CYBER AI 4 ZERO TRUST NETWORK ACCESS (ZTNA) - Intelligent dynamic multi dimensional security approach.
Smart Automation for the complete process. Real time monitoring 2 identify breaches (Alarm React Respond). Intelligent Behavioural Analytics to identify patterns - Erratic Actions through combination of user data + location + user behaviour = Log info 4 future access reference retrieval. If APT breach identified mechanically protect the centralised data vault.

Behavioural Analytics .
Application of complex algorithms to individual level data to derive insights , generate forecasts and make predictions about future human behaviour. Global INTEL Agencies could hypothetically implement AI to make predictions about future behaviour. Major Application - Insider Threat Detection (ITD) - Govt & Military etc.
BA is here to stay. BA techniques may not just be effective in refining assessment of risk but also discovering new leads about evolving cyber threats landscape. Increasingly sophisticated use of AI and BA can be deployed to extract information from bulk datasets.

US Pentagon believes that precognitive AI can predict events 'days in advance' - Global Information Dominance Experiments (GIDE) - AI + CLOUD COMPUTING + SENSORS. Mix of military and civilian sensors to address scenarios where contested logistics might pose a problem. GIDE tech employs ML based system to send fast critical updates and alerts. Can prevent surprise aggression or lead to negotiations instead of conflict . Humans will still be heavily involved in the process.

Complex weapons platforms also coordinate attack or defense among geographically disparate forces. A CyberAttack on these weapons platforms can crash the software used to runthem. That could sideline a fighter jet or radar that protects a aircraft carrier battlegroup or cause a Military satellite to go offline using non kinetic means - Lasers , radio frequency jammers and Cyberattacks . Satellite navigation systems are also at risk of jamming and spoofing. Satellites are also crucial for coordinating electricity grids and time stamping financial transactions. Geolocation is susceptible to electronic interference.

Penetrating communication networks , sabotaging databases (deleting spare engines for fighter jets from spare parts roster) and locking legitimate users out from crucial networks. The NSA wants military industrial complex to take cyber vulnerabilities seriously. Unlike the kinetic battlefield where aircraft drones and armored fighting vehicles spend most of their time out of contact with the enemy - The wireless nature of computer networks means that those same weapons will be under constant threat of enemy assault . And that requires a different kind of armor.

credit - NATIONAL SECURITY AGENCY.

A Supply chain attack is an incredibly expensive operation . Back doors imitate legimitate email users and fool the electronic systems that are supposed to assure identities of users with the right login credentials and additional authentication.
Such an attack has the opportunity to hit a massive quantity of targets but if reached to far the APT would lose their incredible access - FireEye

Complex Weapon systems and platforms are vulnerable to Cyber Attack - Weapon Systems don't just include hypersonic missiles or lasers. There are computers at wings , at sea and on land. We don't think of weapons systems that way but none of them works without computers.These computers add functionality , including fire control (correcting and adjusting aim against distant or fast moving

targets), navigation,(receiving AGPS signals) and
communications (voice and data)

UN Appointed independent rights experts - AI Powered spyware & disinformation is on the rise & regulation of Space has become urgent.AI based biometric surveillance systems are increasingly being
used in sensitive contexts without individuals knowledge or consent.
Urgent & strict regulatory red lines are needed for technologies that claim to perform emotion or gender recognition. The Human Rights Council appointed experts condemned the already alarming use and
impacts of spyware and surveillance technologies on the work of human rights defenders and journalists often under the guise of National security and counter terrorism measures

Human Rights Council also called for regulation to address the lightning fast development of generative AI that's enabling mass production of fake online content which spreads disinformation
and hate speech. Encryption and Privacy are paramount. They underlined the need to ensure technical solutions - including
strong end to end encryption and unfettered access to VPNs - and secure and protect digital communications.

"Adversarial AI" - A Threat to military systems - Shift5's

Lospinoso says - The former Army Captain told a Senate Armed Services panel how AI can impact Military Operations.

Cyber Intelligent Attacks .

1. AI driven Malware - Artificially intelligent malware can infect devices faster than ever before becoming harder to detect targeting more victims and creating more convincing phishing attacks.
2. Vulnerable Applications - Weak application security creates an entry point for APT to infiltrate computer systems. AI can be used to hide malicious code within applications , sometimes programming the attack to execute well after the app has been installed Malicious codes can be present for years before they strike. Data Obfuscation - An image is worth a thousand lines of malware. Malware hidden in images developed by AI can only be detected by AI.
3. Expanded attack surface - Hybrid work and cloud access in personal devices widens the surface are for cyberattacks. AI creates an even more involved that landscape expanding what devices and machines can be used to infiltrate systems.
4. Constant evolution - AI is always evolving. While the benefits include enhanced threat detection. APT are constantly learning from advanced AI tools to develop more advanced attacks and improve their malware. The dawn of Advanced Intelligent Polymorphic cyber attacks is here.

Therefore it's about time to intelligently automate endpoint security , email security , Application security , identity and access management.

Thanks to

1. NORTH ATLANTIC TREATY ORGANISATION.
2. UN APPOINTED INDEPENDENT RIGHTS EXPERTS.
3. INTELLIGENCE AND NATIONAL SECURITY ALLIANCE.
4. NATIONAL SECURITY AGENCY.
5. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.
6. INFORMATION SYSTEMS AND SECURITY ASSOCIATION INTERNATIONAL.
7. EUROPEAN DEFENCE AGENCY.
8. EUROPEAN PARLIAMENTARY RESEARCH SERVICE.

1PowerCyber @ easytech4all.net

https://1powercyber.substack.com

https://1powercyber.blogspot.com

https://easytech4all.tumblr.com

https://linktr.ee/1powercyber

AI impact on cybersecurity -

AI Cyberdefense systems are being implemented to proactively detect and
mitigate threats. Traditional antivirus relies on blacklisting historic threats based on virus signatures. AI based EDR can recognise aspects of software that may be malicious without the need to rely on pre defined database.

MAJOR APPLICATION IN -
EDR - USER AUYHENTICATION - NETWORK DETECTION - INTRUSION
DETECTION AND PREVENTION (IDS) - LOG MANAGEMENT AND SIEM.

Behavioural Biometrics identifies users based on unique aspects of their digital activity - Active authentication systems enhance cybersecurity by ensuring ongoing user authentication

CYBER AI 4 ZERO TRUST NETWORK ACCESS (ZTNA) - Intelligent dynamic multi dimensional security approach.
Smart Automation for the complete process. Real time monitoring 2 identify breaches (Alarm React Respond). Intelligent Behavioural Analytics to identify patterns - Erratic Actions through combination of user data + location + user behaviour = Log info 4 future access reference retrieval. If APT breach identified mechanically protect the centralised data vault.

Behavioural Analytics .
Application of complex algorithms to individual level data to derive insights , generate forecasts and make predictions about future human behaviour. Global INTEL Agencies could hypothetically implement AI to make predictions about future behaviour. Major Application - Insider Threat Detection (ITD) - Govt & Military etc.
BA is here to stay. BA techniques may not just be effective in refining assessment of risk but also discovering new leads about evolving cyber threats landscape. Increasingly sophisticated use of AI and BA can be deployed to extract information from bulk datasets.

US Pentagon believes that precognitive AI can predict
events 'days in advance' - Global Information
Dominance Experiments (GIDE) - AI + CLOUD
COMPUTING + SENSORS. Mix of military and civilian
sensors to address scenarios where contested
logistics might pose a problem. GIDE tech employs

ML based system to send fast critical updates and alerts. Can prevent surprise aggression or lead to negotiations instead of conflict . Humans will still be heavily involved in the process.

Complex weapons platforms also coordinate attack or defense among geographically disparate forces. A CyberAttack on these weapons platforms can crash the software used to runthem. That could sideline a fighter jet or radar that protects a aircraft carrier battlegroup or cause a Military satellite to go offline using non kinetic means . Satellite navigation systems are also at risk of jamming and spoofing. Satellites are also crucial for coordinating electricity grids and time stamping financial transactions. Geolocation is susceptible to electronic interference.

Penetrating communication networks , sabotaging databases (deleting spare engines for fighter jets from spare parts roster) and locking legitimate users out from crucial networks. The NSA wants military industrial complex to take cyber vulnerabilities seriously. Unlike the kinetic battlefield where aircraft drones and armored fighting vehicles spend most of their time out of contact with the enemy - The wireless nature of computer networks means that those same weapons will be under constant threat of enemy assault . And that requires a different kind of armor.

credit - NATIONAL SECURITY AGENCY.

A Supply chain attack is an incredibly expensive operation . Back doors imitate legimitate email users and fool the electronic systems that are supposed to assure identities of users with the right login credentials and additional authentication.
Such an attack has the opportunity to hit a massive quantity of targets but if reached to far the APT would lose their incredible access - FireEye

Complex Weapon systems and platforms are vulnerable to Cyber Attack - Weapon Systems don't just include hypersonic missiles or lasers. There are computers at wings , at sea and on land. We don't think of weapons systems that way but none of them works without computers.These computers add functionality , including fire control (correcting and adjusting aim against distant or fast moving targets), navigation,(receiving AGPS signals) and communications (voice and data)

UN Appointed independent rights experts - AI Powered spyware & disinformation is on the rise & regulation of Space has become urgent.AI based biometric surveillance systems are increasingly being used in sensitive contexts without individuals knowledge or consent.
Urgent & strict regulatory red lines are needed for technologies that claim to perform emotion or gender recognition. The Human Rights Council appointed experts condemned the already alarming use and impacts of spyware and surveillance technologies on the work of human rights defenders and journalists often under the guise of National security and counter terrorism measures

Human Rights Council also called for regulation to address the lightning fast development of generative AI that's enabling mass production of fake online content which spreads disinformation and hate speech. Encryption and Privacy are paramount. They underlined the need to ensure technical solutions - including strong end to end encryption and unfettered access to VPNs - and secure and protect digital communications.

"Adversarial AI" - A Threat to military systems - Shift5's

Lospinoso says - The former Army Captain told a Senate Armed Services panel how AI can impact Military Operations.

Thanks to

1. NORTH ATLANTIC TREATY ORGANISATION.
2. INTELLIGENCE AND NATIONAL SECURITY ALLIANCE.
3. NATIONAL SECURITY AGENCY.
4. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.
5. INFORMATION SYSTEMS AND SECURITY ASSOCIATION INTERNATIONAL.
6. EUROPEAN DEFENCE AGENCY.
7. EUROPEAN PARLIAMENTARY RESEARCH SERVICE.

1PowerCyber @ easytech4all.net

https://linktr.ee/1powercyber

AI Decentralised.

Yes, AI can ever be decentralized. In fact, there are already a number of decentralized AI projects underway.
Decentralized AI is a type of AI that is not controlled by a single entity. Instead, it is distributed across a network of nodes, each of which hosts a portion of the AI model. This makes decentralized AI more resistant to censorship and manipulation, as it is not possible to control all of the nodes in the network.
There are a number of benefits to decentralized AI. First, it is more secure, as it is not possible for a single entity to take control of the entire AI model. Second, it is more private, as data does not have to be shared with a central server. Third, it is more efficient, as AI models can be trained on data that is closer to the source.
There are also a number of challenges to decentralized AI. First, it is more difficult to develop and maintain decentralized AI models. Second, it is more difficult to ensure that all of the nodes in the network are working properly. Third, it is more difficult to scale decentralized AI models to large datasets.
Despite these challenges, decentralized AI is a promising technology with the potential to revolutionize the way we use AI. As the technology matures, we can expect to see more decentralized AI projects being developed and deployed.

Here are some specific examples of decentralized AI projects:
Federated learning: Federated learning is a type of decentralized AI that allows AI models to be trained on data that is held locally on devices. This makes federated learning more privacy-preserving than traditional AI training methods, as data does not have to be shared with a central server.
Blockchain: Blockchain is a distributed ledger technology that can be used to store and share AI models. This makes blockchain a potential platform for decentralized AI, as it can provide a secure and immutable way to store AI models.
Edge computing: Edge computing is a type of computing that brings computation closer to the source of data. This makes edge computing a potential platform for decentralized AI, as it can allow AI models to be trained and deployed on devices that are closer to the data.
I believe that decentralized AI has the potential to revolutionize the way we use AI. By making AI more secure, private, and efficient, decentralized AI can help us to create a more transparent and equitable world.

Are Smartphones reliable edge Computing Devices ?

Smartphones are not engineered to function as reliable edge computing devices in the absence of high-speed internet access or links to cloud networks. Smartphones have limited computing power, memory, storage, and battery life, which can constrain the complexity and efficiency of AI models[1]. Smartphones also rely on network connectivity to communicate with other devices and with the cloud, which can be unstable, intermittent, or unavailable in some scenarios[2]. Therefore, smartphones are not ideal for running intensive edge computing applications that require low latency, high bandwidth, and fast response times. However, smartphones can still perform some basic edge computing tasks, such as data collection, preprocessing, filtering, and encryption[3]. Smartphones can also use built-in sensors, such as accelerometers, gyroscopes, and ambient light sensors, to generate and process data on the go[4]. Smartphones can also leverage technologies such as LIDAR and 5G to enhance their edge computing capabilities in the future..

Source: Conversation with Bing, 9/4/2023
(1) What is Mobile Edge Computing (MEC)? - The Enterprisers Project. https://enterprisersproject.com/article/2021/2/what-mobile-edge-computing-mec.
(2) What is Mobile Edge Computing? | Glossary | HPE. https://www.hpe.com/us/en/what-is/mobile-edge-computing.html.
(3) Which Devices Excel in Edge Computing: Phones, Tablets, or PCs?. https://originstamp.com/blog/which-devices-excel-in-edge-computing-phones-tablets-or-pcs/.
(4) LIDAR and Edge computing: Where do smartphones go next?. https://www.redsharknews.com/lidar-and-edge-computing-where-do-smartphones-go-next.
(5) Getty Images. https://www.gettyimages.com/detail/photo/edge-computing-technology-with-distributed-network-royalty-free-image/1197264259.

Data Quality on Edge Devices .

Data quality on edge devices is important for ensuring reliable and robust AI applications on the edge. There are some ways to improve the data quality on edge devices, such as:

- **Analyze the right data at the edge**: The first step to improving data processing at the edge is focusing on the correct data to process on edge devices. Not all data needs to be processed at the edge, and some data may be better suited for cloud or data center processing. Edge devices should analyze the data that is most relevant, timely, and critical for the application, and filter out the unnecessary or redundant data[3].
- **Investigate data before storing it**: Edge processing is all about removing the time and bandwidth required to send information to the cloud or a data center to process it. However, this also means that edge devices need to store the processed data locally, which can consume valuable memory and storage space. Therefore, edge devices should investigate the data before storing it, and determine whether it is worth keeping, deleting, or sending to the cloud for further analysis[3].
- **Strengthen security**: Edge devices are more vulnerable to cyberattacks, data breaches, or physical tampering, which can compromise the security and privacy of the data and the AI models. Edge devices need to implement strong encryption, authentication, and access control mechanisms to protect the data and the AI models from unauthorized or malicious access[1][2].

Source: Conversation with Bing, 9/4/2023
(1) What are the Best Ways to Improve Data Processing at the Edge?. https://itchronicles.com/big-data/what-are-the-best-ways-to-improve-data-processing-at-the-edge/.
(2) A blockchain-based framework for data quality in edge ... - Springer. https://link.springer.com/article/10.1007/s11704-022-2083-8.
(3) Adaptive Strategy to Improve the Quality of Communication for IoT Edge .... https://ieeexplore.ieee.org/document/9221276/.
(4) What is edge computing? | IBM. https://www.ibm.com/topics/edge-computing.
(5) undefined. https://ieeexplore.ieee.org/servlet/opac?punumber=9217527.

Challenges of using Edge Computing with AI

Some of the challenges of using edge computing with AI are:

- **Poor data quality**: Edge devices may generate noisy, incomplete, or inaccurate data, which can affect the performance and accuracy of AI models. Data quality management and validation are essential for ensuring reliable and robust AI applications on the edge[4].
- **Limited resources**: Edge devices have limited computing power, memory, storage, and battery life, which can constrain the complexity and efficiency of AI models. AI models need to be optimized and compressed to fit the resource constraints of edge devices, without compromising their functionality and quality[1][2].
- **Security and privacy**: Edge devices are more vulnerable to cyberattacks, data breaches, or physical tampering, which can compromise the security and privacy of the data and the AI models. Edge devices need to implement strong encryption, authentication, and access control mechanisms to protect the data and the AI models from unauthorized or malicious access[1][3].
- **Network connectivity**: Edge devices rely on network connectivity to communicate with each other and with the cloud, which can be unstable, intermittent, or unavailable in some scenarios. Edge devices need to be able to operate offline or with low bandwidth, and synchronize with the cloud when possible[1][2]..

Source: Conversation with Bing, 9/4/2023
(1) Edge AI: The Future of Artificial Intelligence and Edge Computing. https://www.itbusinessedge.com/data-center/developments-edge-ai/.
(2) Edge AI Explained: How It Works, Features, Challenges & More. https://www.splunk.com/en_us/blog/learn/edge-ai.html.
(3) Edge Computing and AI for IoT: Opportunities and Challenges. https://ieeexplore.ieee.org/abstract/document/10226787.
(4) Artificial intelligence: a killer app for edge computing?. https://stlpartners.com/articles/edge-computing/artificial-intelligence-a-killer-app-for-edge-computing/.
(5) undefined. https://ieeexplore.ieee.org/servlet/opac?punumber=10226627.
(6) Getty Images. https://www.gettyimages.com/detail/photo/edge-computing-technology-with-distributed-network-royalty-free-image/1197264259.

How Dependent is AI on the Cloud ?

AI and cloud computing have a **mutually beneficial relationship** that enhances each other's capabilities. AI depends on the cloud for accessing the computing resources and infrastructure needed to train and deploy AI models at scale[3]. Cloud computing also provides various services that facilitate AI development, such as serverless computing, batch processing, and container orchestration[3]. On the other hand, cloud computing depends on AI for automating complex tasks, optimizing system performance, and improving user experience[2]. AI can also help cloud computing to provide more secure, reliable, and cost-effective solutions for enterprises[4][5]. Therefore, AI and cloud computing are not independent technologies, but rather **interdependent** ones that work together to drive innovation and efficiency.

Source: Conversation with Bing, 9/4/2023
(1) The Role of AI in Cloud Computing: A Beginner's Guide to Starting a .... https://dev.to/aws-builders/the-role-of-ai-in-cloud-computing-a-beginners-guide-to-starting-a-career-4h2.

(2) The Role of AI in Cloud Computing | Nutanix. https://www.nutanix.com/theforecastbynutanix/technology/ai-in-the-cloud.
(3) Taking AI to the Cloud - Datacenters.com. https://www.datacenters.com/news/artificial-intelligence-in-cloud-computing.
(4) Cloud Computing and the Role of Artificial Intelligence - ONPASSIVE. https://onpassive.com/blog/cloud-computing-role-artificial-intelligence/.
(5) The essential role of AI in cloud technology | TechRadar. https://www.techradar.com/features/the-essential-role-of-ai-in-cloud-technology.

Challenges of using edge computing for AI .

Some of the challenges of using edge computing with AI are:

- **Poor data quality**: Edge devices may generate noisy, incomplete, or inaccurate data, which can affect the performance and accuracy of AI models. Data quality management and validation are essential for ensuring reliable and robust AI applications on the edge[4].
- **Limited resources**: Edge devices have limited computing power, memory, storage, and battery life, which can constrain the complexity and efficiency of AI models. AI models need to be optimized and compressed to fit the resource constraints of edge devices, without compromising their functionality and quality[1][2].
- **Security and privacy**: Edge devices are more vulnerable to cyberattacks, data breaches, or physical tampering, which can compromise the security and privacy of the data and the AI models. Edge devices need to implement strong encryption, authentication, and access control mechanisms to protect the data and the AI models from unauthorized or malicious access[1][3].
- **Network connectivity**: Edge devices rely on network connectivity to communicate with each other and with the cloud, which can be unstable, intermittent, or unavailable in some scenarios. Edge devices need to be able to operate offline or with low bandwidth, and synchronize with the cloud when possible[1][2]..

Source: Conversation with Bing, 9/4/2023
(1) Edge AI: The Future of Artificial Intelligence and Edge Computing. https://www.itbusinessedge.com/data-center/developments-edge-ai/.
(2) Edge AI Explained: How It Works, Features, Challenges & More. https://www.splunk.com/en_us/blog/learn/edge-ai.html.
(3) Edge Computing and AI for IoT: Opportunities and Challenges. https://ieeexplore.ieee.org/abstract/document/10226787.
(4) Artificial intelligence: a killer app for edge computing?. https://stlpartners.com/articles/edge-computing/artificial-intelligence-a-killer-app-for-edge-computing/.
(5) undefined. https://ieeexplore.ieee.org/servlet/opac?punumber=10226627.
(6) Getty Images. https://www.gettyimages.com/detail/photo/edge-computing-technology-with-distributed-network-royalty-free-image/1197264259.

Based on the provided notes on "Fundamental Cybersecurity and AI paradigms," it seems that the main focus is on the integration of artificial intelligence (AI) into cybersecurity practices. The notes cover various aspects of AI in cybersecurity, including its potential, challenges, and impact on the digital landscape. The information encompasses the following key points:

- AI-based cybersecurity tools have emerged to predict and mitigate threats, improve security, and defend against evolving cyber attacks[1].
- AI cybersecurity integrates AI into security protocols to predict, identify, and neutralize potential cyber threats, making it a necessity for organizations of all sizes and industries[2].
- AI has become integral to various industrial automation processes, including cybersecurity, but its adoption has faced challenges such as a lack of trust and cybersecurity concerns[3].
- Trends at the nexus of AI and cybersecurity, such as AI-informed defensive strategies and explainable AI (XAI) models, are fundamentally changing the digital landscape and improving cybersecurity protocols[4].
- AI-powered cybersecurity enables proactive defense mechanisms capable of anticipating and mitigating evolving cyber threats, emphasizing the need for a collaborative human-AI partnership[5].
- AI acts as a powerful catalyst and enabler for cybersecurity, with implications for cyber operations and the need to continually adapt risk management approaches and technology implementation[6].
- The rapid advancement of AI is changing the entire business landscape, requiring decision-makers to consider the role of AI in business operations and mitigate its accelerating cybersecurity threat[7].
- AI is shaping an AI arms race between the security industry and cybercriminals, with a focus on securing legitimate AI systems and addressing the workforce shortage in cybersecurity[8].
- AI and cybersecurity have become protean security disruptors, manifesting into new power paradigms for states and nonstate actors, impacting how power is created and manifesting according to AI algorithms[9].
- AI in cybersecurity is being applied through analytics, automating routine tasks, improving threat detection and response, and providing valuable information to inform cybersecurity decisions[10].
- The potential benefits of AI in cybersecurity include improving threat detection and response, automating routine tasks, and improving the efficiency of cybersecurity operations, while challenges include the potential for hackers to use AI to develop more sophisticated cyber threats[11].
- AI has the potential to provide organizations with smarter and more efficient protection against malicious attacks, but its adoption faces challenges and requires responsible and ethical use[12].

Given the comprehensive coverage of AI in cybersecurity, the notes can be summarized and reformatted to highlight the following key points:
- The emergence of AI-based cybersecurity tools to predict and mitigate threats, improve security, and defend against evolving cyber attacks.
- The integration of AI into security protocols as a necessity for organizations of all sizes and industries.
- The challenges and impact of AI adoption in industrial automation processes, including cybersecurity.
- The trends at the nexus of AI and cybersecurity, emphasizing the need for a collaborative human-AI partnership.
- The implications of AI as a powerful catalyst and enabler for cybersecurity, shaping an AI arms race between the security industry and cybercriminals.
- The protean nature of AI and cybersecurity as new power paradigms for states and nonstate actors, impacting how power is created and manifesting according to AI algorithms.
- The application of AI in cybersecurity through analytics, automating routine tasks, improving threat detection and response, and providing valuable information to inform cybersecurity decisions.
- The potential benefits and challenges of AI in cybersecurity, requiring responsible and ethical use.

The reformatted notes can be presented in a structured and concise manner to facilitate understanding and retention of the key information.

Reformatted Notes: Fundamental Cybersecurity and AI Paradigms
1. Emergence of AI-based Cybersecurity Tools
   - Predict and mitigate threats
   - Improve security
   - Defend against evolving cyber attacks

2. Integration of AI into Security Protocols
   - Necessity for organizations of all sizes and industries

3. Challenges and Impact of AI Adoption in Industrial Automation
   - Emphasis on collaborative human-AI partnership

4. Trends at the Nexus of AI and Cybersecurity
   - Implications of AI as a powerful catalyst and enabler

- Shaping an AI arms race between the security industry and cybercriminals

5. Protean Nature of AI and Cybersecurity
   - New power paradigms for states and nonstate actors
   - Impact on how power is created and manifesting according to AI algorithms

6. Application of AI in Cybersecurity
   - Through analytics, automating routine tasks, and improving threat detection and response

7. Potential Benefits and Challenges of AI in Cybersecurity
   - Requirement for responsible and ethical use

By summarizing and reformatting the notes in this manner, the key information on fundamental cybersecurity and AI paradigms can be effectively conveyed and comprehended.

What specific aspects of the notes would you like to focus on for further summarization and reformatting?

Citations:
[1] Cybersecurity And Artificial Intelligence - New Defense Paradigms - LinkedIn https://www.linkedin.com/pulse/cybersecurity-artificial-intelligence-new-defense-paradigms-ortega
[2] Everything You Need to Know About AI Cybersecurity - HubSpot Blog https://blog.hubspot.com/marketing/ai-cybersecurity
[3] Bridging the Gap: The challenges of AI integration in automation and cybersecurity https://www.industrialcybersecuritypulse.com/networks/bridging-the-gap-the-challenges-of-ai-integration-in-automation-and-cybersecurity/
[4] Emerging Trends at the Nexus of Artificial Intelligence & Cybersecurity | Wilson Center https://www.wilsoncenter.org/blog-post/emerging-trends-nexus-artificial-intelligence-cybersecurity
[5] Unleashing the Power of AI in Cybersecurity: A Paradigm Shift for the Modern Workplace https://www.linkedin.com/pulse/unleashing-power-ai-cybersecurity-paradigm-shift-modern-garbo-ms
[6] A Primer On Artificial Intelligence And Cybersecurity - Forbes https://www.forbes.com/sites/chuckbrooks/2023/09/26/a-primer-on-artificial-intelligence-and-cybersecurity/?sh=266e08b275d2
[7] Opportunities and Challenges of AI and its Impact on Cybersecurity - The Conference Board https://www.conference-board.org/publications/opportunities-and-challenges-of-AI-and-its-impact-on-cybersecurity
[8] The Biggest AI Trends in Cybersecurity - CNET https://www.cnet.com/tech/services-and-software/the-biggest-ai-trends-in-cybersecurity/
[9] New Power Paradigms?: Artificial Intelligence and Cybersecurity as Protean Security Disruptors - Air University https://www.airuniversity.af.edu/JIPA/Display/Article/3019376/new-power-paradigms-artificial-intelligence-and-cybersecurity-as-protean-securi/
[10] Five minute guide to artificial intelligence in cybersecurity - Eviden https://eviden.com/insights/blogs/five-minute-guide-to-artificial-intelligence-in-cybersecurity/
[11] The Benefits And Challenges Of AI In Cyber Security - MetaCompliance https://www.metacompliance.com/blog/data-breaches/benefits-and-challenges-of-ai-in-cyber-security
[12] The Future of AI in Cybersecurity: Are We Ready? - CyberDB https://www.cyberdb.co/the-future-of-ai-in-cybersecurity-are-we-ready/
[13] Artificial intelligence for cybersecurity: Literature review and future research directions https://www.sciencedirect.com/science/article/pii/S1566253523001136
[14] The Use of Artificial Intelligence in Cybersecurity: A Review - IEEE Computer Society https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity/
[15] Implementing AI in Cybersecurity: Challenges and Solutions - LinkedIn https://www.linkedin.com/pulse/implementing-ai-cybersecurity-challenges-solutions
[16] Cybersecurity of AI and Standardisation - ENISA - European Union https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation
[17] Using Artificial Intelligence in Cybersecurity | Balbix https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/
[18] The Role of AI in Cybersecurity: Opportunities and Challenges | - Cybernetic Search https://www.cyberneticsearch.com/blog/the-role-of-ai-in-cybersecurity--opportunities-and-challenges/
[19] The AI and Cybersecurity Handbook – Past the Hype and Onto the ROI - freeCodeCamp https://www.freecodecamp.org/news/ai-and-cybersecurity-handbook/
[20] Artificial Intelligence (AI) Cybersecurity | IBM https://www.ibm.com/ai-cybersecurity
[21] Artificial Intelligence In Cybersecurity: Unlocking Benefits And Confronting Challenges https://www.forbes.com/sites/forbestechcouncil/2023/08/25/artificial-intelligence-in-cybersecurity-unlocking-benefits-and-confronting-challenges/?sh=266430a164cf
[22] AI and Cybersecurity: A New Era | Morgan Stanley https://www.morganstanley.com/articles/ai-cybersecurity-new-era
[23] 4 Top Benefits and Challenges of AI in Cybersecurity - The Next Scoop https://thenextscoop.com/ai-cybersecurity/amp/
[24] The Role of Artificial Intelligence in Cybersecurity - Booz Allen https://www.boozallen.com/s/insight/publication/role-of-artificial-intelligence-in-cyber-security.html
[25] 5 Top AI Challenges in Cybersecurity You shouldn't Overlook - MSys Technologies https://www.msystechnologies.com/blog/5-top-ai-challenges-in-cybersecurity-you-shouldnt-overlook/

By Perplexity at https://www.perplexity.ai/search/5bb07a12-fb01-4cde-b7c0-0041ff40374a?s=m

Internet Lookup -

"The UK Bletchley Declaration on AI"
"US President Executive Order - Data and AI Strategy"
"The US Department of Defense AI Adoption Strategy"

https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

https://www.cisa.gov/ai

https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

Blog for work in progress updates on R&A

https://easytech4all.net

https://easytech4all.net/author/easytechonline/

Cybersec YouTube playlist.

https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADIqTAU2qH-lKcNB-wj

https://1PowerCyber.substack.com

https://1PowerCyber.blogspot.com

https://medium.com/@1PowerCyber

https://easytech4all.tumblr.com

Digital Magazine.

https://flipboard.com/@easytech4all/cybersecurity-6tbejh5oz

https://linktr.ee/1powercyber

https://in.linkedin.com/in/danish-khan-a2b169150

"ARPANET Maps 1969 to 1977". California State University, Dominguez Hills (CSUDH). 4 January 1978. Archived from the original on 19 April 2012. Retrieved 17 May 2012.

Walden, David C. (February 2003). "Looking back at the ARPANET effort, 34 years later". Living Internet. East Sandwich, Massachusetts. Retrieved 19 March 2021.

"Images of ARPANET from 1964 onwards". The Computer History Museum. Retrieved 29 August 2004. Timeline.

"Paul Baran and the Origins of the Internet". RAND Corporation. Retrieved 3 September 2005.

Kleinrock, Leonard. "The Day the Infant Internet Uttered its First Words". UCLA. Retrieved 11 November 2004. Personal anecdote of the first message ever sent over the ARPANET

"Doug Engelbart's Role in ARPANET History". 2008. Retrieved 3 September 2009.

Waldrop, Mitch (April 2008). "DARPA and the Internet Revolution". 50 years of Bridging the Gap. DARPA. pp. 78–85. Archived from the original on 15 September 2012. Retrieved 26 August 2012.

"Robert X Cringely: A Brief History of the Internet". YouTube. Archived from the original on 20 March 2013.

Blog for work in progress updates on R&A

https://easytech4all.net

https://easytech4all.net/author/easytechonline/

Cybersec YouTube playlist.

https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADIqTAU2qH-lKcNB-wj

https://1PowerCyber.substack.com

https://1PowerCyber.blogspot.com

https://medium.com/@1PowerCyber

https://easytech4all.tumblr.com

Digital Magazine.

https://flipboard.com/@easytech4all/cybersecurity-6tbejh5oz

https://linktr.ee/1powercyber

https://in.linkedin.com/in/danish-khan-a2b169150

"ARPANET Maps 1969 to 1977". California State University, Dominguez Hills (CSUDH). 4 January 1978. Archived from the original on 19 April 2012. Retrieved 17 May 2012.

Walden, David C. (February 2003). "Looking back at the ARPANET effort, 34 years later". Living Internet. East Sandwich, Massachusetts. Retrieved 19 March 2021.

"Images of ARPANET from 1964 onwards". The Computer History Museum. Retrieved 29 August 2004. Timeline.

"Paul Baran and the Origins of the Internet". RAND Corporation. Retrieved 3 September 2005.

Kleinrock, Leonard. "The Day the Infant Internet Uttered its First Words". UCLA. Retrieved 11 November 2004. Personal anecdote of the first message ever sent over the ARPANET

"Doug Engelbart's Role in ARPANET History". 2008. Retrieved 3 September 2009.

Waldrop, Mitch (April 2008). "DARPA and the Internet Revolution". 50 years of Bridging the Gap. DARPA. pp. 78–85. Archived from the original on 15 September 2012. Retrieved 26 August 2012.

"Robert X Cringely: A Brief History of the Internet". YouTube. Archived from the original on 20 March 2013.

Blog for work in progress updates on R&A

https://easytech4all.net

https://easytech4all.net/author/easytechonline/

Cybersec YouTube playlist.

https://youtube.com/playlist?list=PLf-aX7Sa0eCRYUADIqTAU2qH-lKcNB-wj

https://1PowerCyber.substack.com

https://1PowerCyber.blogspot.com

https://medium.com/@1PowerCyber

https://easytech4all.tumblr.com

Digital Magazine.

https://flipboard.com/@easytech4all/cybersecurity-6tbejh5oz

https://linktr.ee/1powercyber

https://in.linkedin.com/in/danish-khan-a2b169150

What are the UN guidelines to curb mis/dis information ?

The UN has put forward several guidelines to curb misinformation and disinformation, aiming to promote international cooperation and protect human rights and fundamental freedoms. These guidelines include:

1. Building societal resilience and media and information literacy through lasting investment.
2. Encouraging companies to respect human rights, conduct human rights due diligence, increase transparency around their policies and practices relating to disinformation, engage with civil society, provide access to researchers, and grant users greater control of their online experiences.
3. Mitigating disinformation and misinformation at scale by internet communications companies through transparency, accountability, accessibility, and cooperation.
4. Protecting freedom of expression while strengthening communities' resilience to the threats posed by mis- and disinformation.
5. Countering misinformation and disinformation in crisis settings to prevent social divisions and mistrust in public institutions.

These guidelines emphasize the importance of transparency, accountability, and cooperation in countering misinformation and disinformation, while also highlighting the need to protect freedom of expression and promote media and information literacy.

Guidelines to Curb Mis/Disinformation by the UN
1. Building societal resilience and media and information literacy through lasting investment.
2. Encouraging companies to respect human rights, conduct human rights due diligence, increase transparency, engage with civil society, and grant users greater control of their online experiences.
3. Mitigating disinformation and misinformation at scale by internet communications companies through transparency, accountability, accessibility, and cooperation.
4. Protecting freedom of expression while strengthening communities' resilience to the threats posed by mis- and disinformation.
5. Countering misinformation and disinformation in crisis settings to prevent social divisions and mistrust in public institutions.

These guidelines aim to promote international cooperation, protect human rights, and combat the spread of misinformation and disinformation.

Citations:
[1] Countering Disinformation - the United Nations https://www.un.org/en/countering-disinformation
[2] 5 ways the UN is fighting 'infodemic' of misinformation - the United Nations https://www.un.org/en/un-coronavirus-communications-team/five-ways-united-nations-fighting-%E2%80%98infodemic%E2%80%99-misinformation
[3] [PDF] Shared UN considerations for online communications companies on the issues of countering disinformation and enhancing transparency - the United Nations https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/general/UN_InteragencyDialogue2_v2.pdf
[4] Freedom of expression is key to countering disinformation | OHCHR https://www.ohchr.org/en/stories/2022/11/freedom-expression-key-countering-disinformation
[5] Tackling mis- and disinformation: Seven insights for UN peace operations | SIPRI https://www.sipri.org/commentary/blog/2023/tackling-mis-and-disinformation-seven-insights-un-peace-operations
[6] RISE ABOVE: Countering misinformation and disinformation in the crisis setting | United Nations Development Programme https://www.undp.org/eurasia/dis/misinformation

By Perplexity at https://www.perplexity.ai/search/b91cf285-7853-42a1-9b65-a1cca2027c5b?s=m

The United Nations (UN) has a number of guidelines to curb mis/disinformation, including:

* **Protect freedom of expression.** The UN recognizes that freedom of expression is a fundamental human right, and that any restrictions on this right must be necessary and proportionate. However, the UN also recognizes that there are limits to freedom of expression, such as when it is used to spread hate speech or incite violence.
* **Promote media literacy and critical thinking.** The UN believes that it is important for people to be able to identify and evaluate information critically, in order to be able to distinguish between fact and fiction. The UN supports initiatives to promote media literacy and critical thinking, such as educational programs and training for journalists.
* **Support fact-checking and debunking.** The UN supports efforts to fact-check and debunk misinformation, such as the work of fact-checking organizations and social media platforms.
* **Promote transparency and accountability.** The UN believes that it is important for people to know who is producing and spreading misinformation, and to hold them accountable. The UN supports efforts to promote transparency and accountability, such as requiring social media platforms to disclose information about political advertising and to remove accounts that are spreading misinformation.
* **Address the root causes of mis/disinformation.** The UN believes that it is important to address the root causes of mis/disinformation, such as poverty, inequality, and lack of access to education. The UN supports initiatives to address these issues, such as promoting sustainable development and inclusive societies.

In addition to these general guidelines, the UN has also developed specific guidelines for tackling mis/disinformation in the context of elections, pandemics, and other crises.

Here are some examples of how the UN is working to implement these guidelines:

* **UNESCO** is working with governments, media organizations, and civil society groups to promote media literacy and critical thinking, support fact-checking and debunking, and promote transparency and accountability.
* **WHO** is working to counter misinformation about COVID-19 and other public health issues.
* **UNDP** is working to build resilience to mis/disinformation in conflict and post-conflict settings.

* **The UN Secretary-General's High-level Panel on Digital Cooperation** has developed a number of recommendations for tackling mis/disinformation, including the establishment of a global fund to support fact-checking and debunking, and the creation of a global code of conduct for social media platforms.

The UN's guidelines on mis/disinformation are still under development, as the UN continues to learn more about this complex and evolving issue. However, the UN's commitment to addressing mis/disinformation is clear, and the UN is working with a wide range of partners to implement its guidelines and make the internet a safer and more reliable source of information for everyone.

how can ai tools be integrated into existing cybersecurity infrastructure

Integrating AI tools into existing cybersecurity infrastructure presents both opportunities and challenges. Here are some best practices and considerations for effectively integrating AI into cybersecurity:

Best Practices for Integrating AI into Cybersecurity
1. **Assess Cybersecurity Needs**: Before integrating AI, assess the types of cyber threats and vulnerabilities in your systems to determine the type of AI technology needed[11].
2. **Select the Right AI Technology**: Choose AI technologies such as machine learning, deep learning, and natural language processing that align with your cybersecurity needs[11].
3. **Train Staff on AI Tools**: Provide comprehensive training on how AI-based security tools work and how to use them effectively, including cybersecurity best practices and the latest cyber threats[11].
4. **Monitor and Improve**: Continually monitor and improve your cybersecurity strategy to ensure the effective integration of AI-based security tools[11].

Considerations for Integrating AI into Cybersecurity
1. **Data Privacy**: Protect sensitive data when using AI systems by handling data securely to prevent breaches[9].
2. **False Positives**: AI-powered security systems can sometimes generate false positives, leading to unnecessary alerts and strain on resources. Balancing accuracy and false positives is essential[9].
3. **Adversarial Attacks**: Implement robust defense mechanisms against adversarial attacks, as cybercriminals may attempt to manipulate AI systems[9].
4. **Ethical Considerations**: Address ethical concerns such as privacy, bias, and accountability when using AI in cybersecurity[6].

Challenges of AI Integration in Cybersecurity
1. **Lack of Trust**: Some organizations may experience challenges due to a lack of trust from the C-suite down to the operational level when integrating AI technologies into existing systems[1].
2. **Cybersecurity Concerns**: Concerns about cybersecurity, including potential misuse or abuse of AI, can pose challenges when integrating AI into existing cybersecurity infrastructure[1][3].

By following best practices and considering the associated challenges, organizations can effectively integrate AI tools into their existing cybersecurity infrastructure, enhancing their security posture and response capabilities.

For further details on the challenges and solutions in implementing AI in cybersecurity, please refer to the provided search results.

Citations:
[1] Bridging the Gap: The challenges of AI integration in automation and cybersecurity https://www.industrialcybersecuritypulse.com/networks/bridging-the-gap-the-challenges-of-ai-integration-in-automation-and-cybersecurity/
[2] Best practices in cybersecurity for AI - Tarlogic https://www.tarlogic.com/blog/best-practices-cybersecurity-ai/
[3] The Benefits And Challenges Of AI In Cyber Security - MetaCompliance https://www.metacompliance.com/blog/data-breaches/benefits-and-challenges-of-ai-in-cyber-security
[4] AI in Cyber Security: Pros and Cons, and What it Means for Your Business https://terranovasecurity.com/blog/ai-in-cyber-security/
[5] AI Best Practices: Securely Use Tools like ChatGPT - Infosec Resources https://resources.infosecinstitute.com/topics/security-awareness/ai-best-practices/
[6] The Benefits and Challenges of AI in Cybersecurity: Finding the Balance - LinkedIn https://www.linkedin.com/pulse/benefits-challenges-ai-cybersecurity-finding-balance
[7] Everything You Need to Know About AI Cybersecurity - HubSpot Blog https://blog.hubspot.com/marketing/ai-cybersecurity
[8] Discover The Best AI Tools: Best Practices To Use It Safely - SSL2BUY https://www.ssl2buy.com/cybersecurity/ai-tools-best-practices-to-use-safely
[9] Implementing AI in Cybersecurity: Challenges and Solutions - LinkedIn https://www.linkedin.com/pulse/implementing-ai-cybersecurity-challenges-solutions
[10] The AI Race for Industrial Cybersecurity - Towards AI https://towardsai.net/p/machine-learning/the-ai-race-for-industrial-cybersecurity
[11] How to Integrate AI into Your Cybersecurity Strategy - Cyber Security Solutions, Compliance, and Consulting Services https://www.infoguardsecurity.com/how-to-integrate-ai-into-your-cybersecurity-strategy/
[12] The Role of AI in Cybersecurity: Opportunities and Challenges | - Cybernetic Search https://www.cyberneticsearch.com/blog/the-role-of-ai-in-cybersecurity--opportunities-and-challenges/
[13] Using Artificial Intelligence in Cybersecurity | Balbix https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/
[14] Best Practices for Implementing AI in Cybersecurity Threat Hunting - LinkedIn https://www.linkedin.com/pulse/best-practices-implementing-ai-cybersecurity-threat-nalinakshan
[15] Assessing the pros and cons of AI for cybersecurity - Security Magazine https://www.securitymagazine.com/articles/99487-assessing-the-pros-and-cons-of-ai-for-cybersecurity
[16] The Role of AI in Cybersecurity - Cyber Defense Magazine https://www.cyberdefensemagazine.com/the-role-of-ai-in-cybersecurity/
[17] How Security Analysts Can Use AI in Cybersecurity - freeCodeCamp https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/
[18] 4 Top Benefits and Challenges of AI in Cybersecurity - The Next Scoop https://thenextscoop.com/ai-cybersecurity/amp/
[19] The AI and Cybersecurity Handbook – Past the Hype and Onto the ROI - freeCodeCamp https://www.freecodecamp.org/news/ai-and-cybersecurity-handbook/
[20] Mastering The Challenges Of AI: Privacy, Security And Compliance Strategies - Forbes https://www.forbes.com/sites/forbestechcouncil/2023/08/18/mastering-the-challenges-of-ai-privacy-security-and-compliance-strategies/?sh=266464a170e6
[21] Artificial Intelligence: Confronting challenges in cybersecurity - Opinions & Blogs News https://www.wionews.com/opinions-blogs/artificial-intelligence-confronting-challenges-in-cybersecurity-614139
[22] The Impact of AI on Cybersecurity - IEEE Computer Society https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity/

By Perplexity at https://www.perplexity.ai/search/15a51b3d-d90f-49fe-bcae-21c46962af94?s=m

what are some examples of ai tools used in cybersecurity

Some examples of AI tools used in cybersecurity include:

1. **Sophos Intercept X**: This tool offers instant visibility and advanced threat detection across various areas such as Cloud, Apps, Email, Endpoint, Network, Zero Trust, and OT[3].

2. **Symantec Endpoint Security**: This platform features machine learning exploit and malware prevention, using AI to look for and prevent threats[3].

3. **Splunk User Behavior Analytics**: This tool provides advanced threat detection and prediction, allowing organizations to understand and respond to emerging threats in real-time[3].

4. **Vectra Cognito**: This AI tool detects and responds to attacks inside the cloud, data center, IoT, and enterprise networks, using human intelligence and data science for faster threat detection and real-time automation[7].

5. **Darktrace**: Darktrace is an AI-powered cybersecurity platform that utilizes machine learning and AI algorithms to detect and respond to cyber threats[4].

6. **Trellix**: This tool offers advanced threat detection and prediction, allowing organizations to predict and prevent emerging threats, identify root causes, and respond in real-time[3].

7. **Tenable Nessus**: This AI tool provides vulnerability management and prioritization, responding to incidents before hackers exploit vulnerabilities[3].

8. **Securonix**: This tool harnesses the potential of machine learning, automation, and data analytics to provide a deeper understanding of an organization's IT infrastructure, enhancing audit capabilities[3].

9. **IBM Watson for Cyber Security**: This tool uses AI to transform security from a reactive to a predictive approach, defending against possible threats and cyber attacks[8].

These AI tools leverage artificial intelligence, machine learning, and advanced analytics to provide proactive and effective protection against cyber attacks, offering enhanced threat detection capabilities, improved incident response, and reduced manual efforts for security teams[4][8].

Citations:
[1] The Most Useful Tools for AI & Machine Learning in Cybersecurity | HostPapa Blog https://www.hostpapa.com/blog/web-hosting/the-most-useful-tools-for-ai-machine-learning-in-cybersecurity/
[2] AI Applications in Cybersecurity with Real-Life Examples - AltexSoft https://www.altexsoft.com/blog/ai-cybersecurity/
[3] 5 AI Tools for IT and Cybersecurity Audits - LinkedIn https://www.linkedin.com/pulse/5-ai-tools-cybersecurity-audits-priya-ranjani-mohan
[4] 9 Best AI Security Tools Of 2023 - Wbcom Designs https://wbcomdesigns.com/best-ai-security-tools/
[5] AI in Cybersecurity: 5 Crucial Applications - V7 Labs https://www.v7labs.com/blog/ai-in-cybersecurity
[6] 9 Best AI Security Tools of 2023 - Renaissance Rachel https://renaissancerachel.com/best-ai-security-tools/
[7] Top Artificial Intelligence-Based Tools For Cyber Security - MarkTechPost https://www.marktechpost.com/2022/08/11/top-artificial-intelligence-based-tools-for-cyber-security/
[8] Artificial intelligence in cybersecurity tools - Next IT Security https://nextitsecurity.com/artificial-intelligence-in-cybersecurity-tools/

By Perplexity at https://www.perplexity.ai/search/1e817821-e758-4ab7-82bc-89f8fa00128d?s=m

what are the benefits of using ai in cybersecurity

The benefits of using AI in cybersecurity are numerous and impactful. Here are some key advantages:

1. **Faster Threat Detection and Response**: AI can detect, analyze, and respond to security threats faster than traditional methods. It can sift through vast amounts of data to identify abnormal behavior and detect malicious activity, such as new zero-day attacks, automating security processes like patch management, and improving response time to attacks[3].

2. **Improved Accuracy and Efficiency**: AI-based cybersecurity systems provide improved accuracy and efficiency compared to traditional security solutions. AI algorithms can recognize patterns that may be difficult for humans to spot, leading to more accurate detection of malicious activity. Furthermore, AI can automate tedious security tasks, freeing valuable resources to focus on other business areas[3].

3. **Consistent Protection 24/7**: AI and cybersecurity are an ideal combination for monitoring network security around the clock, providing consistent protection against security threats[8].

4. **Handling Large Volumes of Data**: AI has the ability to process enormous volumes of data with assembly-line efficiency, automating the creation of algorithms to detect security threats across a wide range of elements in the IT network[8].

5. **Identifying Unknown Threats**: AI can effectively identify and prevent unknown threats, which can cause severe damage if undetected, leveling the playing field against attackers and enhancing protection[2].

6. **Automation of Time-Consuming Tasks**: AI can automate time-consuming and repetitive tasks, such as monitoring, analyzing events, predicting outcomes, taking preventive actions, and generating alerts of suspicious behaviors for human review, all of which can be done continuously in real time[4].

7. **Enhanced Scalability and Cost Savings**: AI can automate tedious security tasks, freeing valuable resources to focus on other business areas, and identify malicious activity by automating routine tasks, providing valuable information to inform cybersecurity decisions[3][7].

These benefits highlight the significant advantages of integrating AI into cybersecurity practices, improving threat detection, response, and overall security posture.

Citations:
[1] Evaluate the risks and benefits of AI in cybersecurity | TechTarget https://www.techtarget.com/searchenterpriseai/tip/Evaluate-the-risks-and-benefits-of-AI-in-cybersecurity
[2] Top 10 Uses of AI for Cybersecurity (+14 Applications) - Engati https://www.engati.com/blog/ai-for-cybersecurity
[3] AI in Cyber Security: Pros and Cons, and What it Means for Your Business https://terranovasecurity.com/blog/ai-in-cyber-security/
[4] Using AI In Cybersecurity: Exploring The Advantages And Risks - Forbes https://www.forbes.com/sites/forbestechcouncil/2023/09/18/using-ai-in-cybersecurity-exploring-the-advantages-and-risks/?sh=266e08a129c7
[5] AI in Cyber Security: Use Cases, Advantages - KnowledgeHut https://www.knowledgehut.com/blog/security/ai-in-cyber-security
[6] Assessing the pros and cons of AI for cybersecurity - Security Magazine https://www.securitymagazine.com/articles/99487-assessing-the-pros-and-cons-of-ai-for-cybersecurity
[7] The Benefits And Challenges Of AI In Cyber Security - MetaCompliance https://www.metacompliance.com/blog/data-breaches/benefits-and-challenges-of-ai-in-cyber-security
[8] The Benefits of Cybersecurity Powered by Artificial Intelligence - NIC Inc. https://www.nicitpartner.com/benefits-cybersecurity-powered-artificial-intelligence/

By Perplexity at https://www.perplexity.ai/search/0e6d9206-2620-47bf-8d7e-d22d455966c7?s=m

https://www.nato.int/docu/review/articles/2023/06/06/nato-and-strategic-competition-in-cyberspace/index.html

https://defensescoop.com/2023/07/14/pentagon-testing-generative-ai-in-global-information-dominance-experiments/

https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

https://www.c4isrnet.com/artificial-intelligence/2023/11/02/pentagon-debuts-new-data-and-ai-strategy-after-biden-executive-order/#:~:text=WASHINGTON%20%E2%80%94%20The%20U.S.%20Department%20of,and%20autonomous%20technologies%20including%20drones

https://www.military.com/defensetech/2019/02/13/pentagon-wants-use-ai-predict-next-wildfire-or-earthquake.html/amp

https://www.britannica.com/technology/warning-system/Electromagnetic-sensors

https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=en

https://www.cisa.gov/ai

Artificial general intelligence (AGI) is a hypothetical type of intelligent agent that could learn to accomplish any intellectual task that human beings or animals can perform[3]. AGI could enable seamless future military operations by enhancing the following aspects:

- Strategy and Artificial Intelligence: AGI could help military leaders formulate and implement effective strategies that take into account various factors, such as the adversary's capabilities, intentions, and vulnerabilities, as well as the political, legal, and ethical implications of military actions[1].
- Doctrine and Artificial Intelligence: AGI could help military organizations develop and update their doctrines, which are the principles and guidelines that govern the conduct of military operations. AGI could also help train and educate military personnel on how to apply these doctrines in different scenarios[1].
- Plans and Artificial Intelligence: AGI could help military planners create and execute detailed plans for specific military operations, such as campaigns, missions, or tasks. AGI could also help monitor and adjust these plans in real time, based on the changing situation and feedback from the field[1].
- Rules of Engagement and Artificial Intelligence: AGI could help military commanders and operators comply with the rules of engagement (ROE), which are the legal and ethical constraints that regulate the use of force in military operations. AGI could also help verify and validate the ROE, as well as identify and report any violations or breaches[1].
- Orders and Artificial Intelligence: AGI could help military commanders and operators communicate and execute orders, which are the instructions and directives that specify the objectives, tasks, and actions of military operations. AGI could also help coordinate and synchronize the actions of different units and platforms, as well as provide feedback and assessment of the results[1].

These are some of the ways that AGI could enable seamless future military operations. However, there are also many risks and challenges associated with the development and use of AGI for military purposes, such as ethical, legal, and social issues, as well as the potential for misuse, abuse, or hacking by malicious actors[2]. Therefore, it is important to ensure that AGI systems are designed, deployed, and governed in a responsible and accountable manner, with respect for human dignity, rights, and values.

Source: Conversation with Bing, 1/12/2024
(1) Artificial general intelligence - Wikipedia. https://en.wikipedia.org/wiki/Artificial_general_intelligence.
(2) From Strategy to Orders: Preparing and Conducting Military Operations .... https://dam.gcsp.ch/files/misc/military-operations-working-paper-v2.
(3) AGI Is Ready To Emerge (Along With The Risks It Will Bring) - Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/07/27/agi-is-ready-to-emerge-along-with-the-risks-it-will-bring/.

AGI: A Potential Key to Humanity's Most Challenging Problems
Artificial General Intelligence (AGI) holds immense potential to tackle some of the most complex problems facing humanity. Its ability to learn, reason, and adapt could be instrumental in finding solutions that elude our current capabilities. Here's how AGI might make a difference:
Data-Driven Insights:
Climate Change: AGI can analyze vast datasets on climate patterns, emissions, and renewable energy technologies. This could lead to improved climate models, prediction of extreme weather events, and development of efficient sustainability solutions.
Disease Outbreaks: AGI can analyze genetic data, track disease spread in real-time, and optimize resource allocation during pandemics. It could also support the development of personalized medicine and accelerated drug discovery.
Global Challenges: AGI can analyze complex economic and social data to identify and address issues like poverty, hunger, and inequality. It can also help optimize resource allocation in developing countries and support disaster relief efforts.
Beyond Data:
Creativity and Innovation: AGI can break through conventional thinking patterns and generate novel solutions in fields like science, engineering, and art. Imagine it designing next-generation materials, optimizing energy production, or composing groundbreaking music.
Decision-Making and Policy Planning: AGI can analyze complex scenarios and predict the potential outcomes of different policy decisions. This can lead to more informed and evidence-based governance, improving resource allocation and social welfare.
Human-AGI Collaboration: AGI can act as a powerful tool to augment human capabilities, enhancing learning, communication, and problem-solving. Imagine doctors assisted by AGI for diagnosis or teachers supported by adaptive learning platforms powered by AGI.
Hypothetical Simulations:
While AGI remains in its early stages, researchers are exploring hypothetical simulations to understand its potential impact. Some examples include:
The Blue Brain Project: Aims to digitally reconstruct the human brain and simulate its functions. This could provide insights into consciousness, intelligence, and neurological diseases.
The OpenWorm Project: Aims to create a complete digital model of the C. elegans worm, allowing researchers to virtually experiment with its biology and behavior.
The Global Brain Hypothesis: Proposes a future where AGIs are interconnected and form a collective intelligence capable of solving complex global problems.
Links and Sources:
AGI and Climate Change: https://www.scribd.com/document/268809745/The-AI-Revolution-Road-to-Superintelligence-Wait-But-Why-pdf
AGI and Disease Outbreaks: https://pubmed.ncbi.nlm.nih.gov/37655671/
AGI and Global Challenges: https://www.businessinsider.com/agi-could-be-worth-trillions-dollars-2030s-ex-meta-exec-2023-2
The Blue Brain Project: https://www.epfl.ch/research/domains/bluebrain/
The OpenWorm Project: https://openworm.org/
The Global Brain Hypothesis: https://en.wikipedia.org/wiki/Global_brain
Remember: AGI is a powerful tool with ethical considerations. Developing and implementing it responsibly will be crucial to ensure its benefits outweigh the risks. As we delve deeper into AGI research, these hypothetical simulations can guide us towards a future where technology empowers humanity to overcome its most pressing challenges.

End of document